Socio-Economic Services for European Research Projects (SESERV)

European Seventh Framework Project FP7-2010-ICT-258138-CSA

Deliverable D3.1
First Report on Social Future Internet Coordination Activities

The SESERV Consortium

University of Zürich, UZH, Switzerland
University of Southampton, IT Innovation Centre, U.K.
Athens University of Economics and Business - Research Center, AUEB-RC, Greece
University of Oxford, UOX, U.K.
Alcatel Lucent Bell Labs, ALBLF, France
ATOS Origin, AOSAE, Spain

For more information on this document or the SESERV support action, please contact:

Prof. Dr. Burkhard Stiller
Universität Zürich, CSG@IFI
Binzmühlestrasse 14
CH—8050 Zürich
Switzerland

Phone: +41 44 635 4355
Fax: +41 44 635 6809
E-mail: info@seserv.org

Document Control

Title: First Report on Social Future Internet Coordination Activities

Type: Internal

Editor(s): Michael Boniface, J. Brian Pickering

E-mail: mjb@it-innovation.soton.ac.uk, jbp@it-innovation.soton.ac.uk

Author(s): Michael Boniface, J. Brian Pickering, (IT Innovation)
Eric Meyer, Cristobal Cobo, Anne-Marie Oostveen (UoX)
Burkhard Stiller, Martin Waldburger (UZH)

Doc ID: D3.1-v1.5.doc

AMENDMENT HISTORY

Version	Date	Author	Description/Comments
V1.0	19th August 2011	Michael Boniface and Brian Pickering	Initial Version
V1.1	28th August 2011	Brian Pickering	Completed main draft (excl Conclusions and Exec Summary)
V1.2	9th September 2011	Michael Boniface	Various updates for consistency with other SESERV deliverables
V1.3	13th September 2011	Michael Boniface	Updates to the FI ecosystem section, conclusions and exec summary
V1.4	14th September 2011	Eric T. Meyer	Final edit
V1.5	2 October 2011	Michael Boniface, Brian Pickering	Updated for public release

Table of Contents

List of Figures

List of Tables

(This page is left blank intentionally.)

1 Executive Summary

This document is Deliverable D3.1 “First Report on Social Future Internet Coordination Activities” of Work Package 3 “Social Future Internet Coordination Activities” within the ICT SESERV Project 258138. The report provides the FISE (Future Internet Socio-Economics) community and the European Commission with the results of co-ordination activities for the societal aspects of the Future Internet (FI) over the period August 2010 to September 2011. The purpose is to discuss societal issues which affect the development and success of FI technologies based on the collective thoughts and opinions of social scientists and technologists working on FI research in EC Challenge 1 and beyond.

The Internet pervades our lives, professionally, commercially and within the context of our personal and leisure activities. The proliferation of uses and involvement online is hugely significant for Europe and the rest of the world. The FI Ecosystem is now a complex and dynamic socio-economic space. There is a significant increase in the diversity of roles, an increased emphasis on users, and a blurring of roles between major market players. The concerns of the Internet have moved from structures purely targeting transit and delivery of data to socio-economic structures supporting exchange of information and knowledge according to the values of individuals and communities.

There are many societal concerns within the FI ecosystem that emerge as a consequence of FI R&D efforts. Six concerns are discussed in detail considering technical innovation, barriers for adoption and future strategies. Topics covered include:

- **Risk Management - Security of Communications**: Risk-management with respect to common infrastructures used for the delivery of services, i.e. clouds and sensor networks. Distribution of control, responsibility and liability in infrastructures. Access to risk expertise. Lack of capacity to assess risks.
- **Privacy**: Erosion of choice and control due to increasing asymmetry between consumers and mega providers. Unauthorised reuse of personal data. Complexity of decision making when accessing services. Fundamental Human Rights.
- **Online Identity**: Diverging definitions of identity. Society conceives stable identity but online identify is inherently dynamic. Relationship between online identity and data.
- **Internet of Things**: Tension between public perceptions and the potential of the technology. Need to engage with ethics and privacy experts.
- **Online Communities**: Service providers are dictating how communities interact and what happens to their data. Communities want to control and define how to maintain community health.
- **Cloud Computing**: Little common understanding of what clouds are. Europe slow to embrace the full potential of cloud computing, focusing more on concerns rather than benefits. Playing catch up with regard to business models and regulatory frameworks.

Based on the discussion of societal concerns eight cross-cutting societal priorities for the FI R&D are presented:

- 1.1. Call for increased transparency (data use and systems)
- 1.2. Call for more user-centricity and control
- 1.3. Continuing need for further multi-disciplinary and cross-sectorial bridging

- 1.4. Striking balances between outer-poles in debates and design
- 1.5. Facilitating further digital literacy development
- 1.6. Addressing lack of common vocabularies and definitions
- 1.7. Need for clarifying digital rights (including digital choice)
- 1.8. Inviting global regulatory frameworks

The Digital Agenda is summarized and how the FI and societal priorities can address obstacles of societal relevance. One key result of engaging with the FI community is identifying that the Digital Agenda is not deeply understood by technologists. There is a gap between a set of high level policies and incentives that are particularly focused on infrastructure and complex regulatory processes. It seems that these regulations ignore some of the citizenship concerns and there is a clear disconnection in this instrument. From discussions with Challenge 1 projects it appears that not even the 'stakeholders' of the Future Internet are fully aware or even interested in the Digital Agenda. The EU Commission needs to find the way to design and update a Digital Agenda that answers to the necessities of a broad spectrum of people and communities (not only the big organizations, companies or government). For instance, the rural and remote regions, the non-organized communities and even SMEs seem to be underrepresented in this 2020 policy action.

Since SESERV was conceptualised significant societal, economic and environmental events continue to pose huge challenges. Economic progress is not delivering an increased quality of life and new value structures that consider qualitative measures may be needed to provide incentives for societal behaviour change. Such visions are attractive but there appears to be no credible and desirable vision for a sustainable future. With the tension between the common good and private interest (as embodied by the net neutrality debate) routes to sustainable socio-economic structures that offer trust and opportunity for all are not clear.

In this context, the goals of SESERV remain highly relevant. Maintaining focus on assisting technologists in their understanding of the potential broader impacts of FI technology along with barriers and strategies for adoption through dialogue with social scientists is increasingly important. The challenges facing society are larger than ever and the Future Internet will surely be an integral part of possible solutions. However, to realise the benefits all stakeholders will need to engage in discourse between those that study and those that build the Future Internet.

2 Introduction

The relationship between technology and society is complex. It may be tempting to see technology and society as one and the same[1]: there is no society without the enabling technologies that allow us to prosper; and there is no technology without the pull of a society eager to explore new ways of doing things. This may, however, be an oversimplification as it largely depends on who we listen to and what they choose to tell us.

Technology constrains what society does by often deliberately limiting the choice of possible technologies are on offer. However, we need to take some responsibility and accept that choices are always possible; we must think critically about what technologies we adopt, rather than accepting them and taking for granted that others can and do make the choice for us. We really need to look at and consider behaviour patterns, and encourage interactions between users and technologists to mutually shape future technology[2].

Innovation is largely serendipitous; for maximum benefit, the complex interactions and even antagonisms between society and the technologists need to be nurtured in a suitable and enabling environment. In truth, social (what are the pressing needs of users), legal (what are the norms we expect to be respected) and technical (what is actually possible at this time) perspectives combine to create the technologies we develop, although even then we should be aware that how we think and perceive society – our cognitive awareness – will shape the choices we make[3].

The interactions between technologists, society, legislation and regulation are key drivers in how the Future Internet (FI) and associated applications and services will develop. In this deliverable we report on the societal aspects of the FI from the perspectives of both social scientists and technologists involved in EC projects within Challenge 1 responsible for making the Future Internet a reality.

2.1 Purpose of D3.1

The report provides the FISE community and the EC with the results of co-ordination activities for the societal aspects of the FI over the period August 2010 to September 2011. The purpose is to discuss societal issues which affect the development and success of FI technologies based on the collective thoughts and opinions of social scientists and technologists (See Section 8) working on FI research in EC Challenge 1 and beyond[4].

The document aims to bring together the outcomes of engagements with the FI community. This includes a survey of projects, Future Internet Assembly (FIA) sessions, a cross-disciplinary SESERV workshop and direct engagement with a selected number of FP7 projects. Support studies, which highlight both social economic considerations for a digital Europe, are also considered.

---

[1] Chrysanthi Papoutsi (2011) Break-out session Privacy. SESERV Oxford Workshop, June 2011. http://www.seserv.org/panel/SESERV_privacy.pdf

[2] SESERV Oxford Workshop, June 2011, Debate Will the Design of the Future Internet be driven by Technology or Societal Concerns http://www.seserv.org/panel/conferences-webcasts#debate

[3] Concepts like ‘social’ or ‘users’ are often confusing in a complex multistakeholder system. Throughout this document the term “user” indicates a matter of perspective in relation to a technology and not a specific stakeholder role (e.g. a citizen)

[4] http://cordis.europa.eu/fp7/ict/programme/challenge1_en.html

The goal is to highlight challenges and priorities within the FI ecosystem and to raise awareness of how these challenges can affect societal challenges posed by the Digital Agenda.

2.2 Document Scope

This document is Deliverable D3.1 First Report on Social Future Internet Coordination Activities for the ICT SESERV Project.

Section 3 discusses the societal aspects of the FI ecosystem considering key societal concerns associated with security, privacy, identity, Internet of Things, online communities and cloud computing. The Internet landscape is explored, terms (Section 3.1) and the emerging stakeholders within the FI ecosystem are described (Section 3.2) building on the Tussle analysis work conducted in SESERV's economic activities[5]. The societal concerns, challenges and potential strategies are discussed (Section 3.3) and a cross-cutting set of societal priorities for FI research identified (Section 3.4).

Section 4 discusses how the FI community can better address societal obstacles identified in the Digital Agenda[6]. The goals and objectives of Digital Agenda are summarized in Section 4.1 and the related societal obstacles discussed in Section 4.2. The technologists' perspectives on the Digital Agenda from members of the FI community are presented in Section 4.3. Finally, Section 5 provides conclusions and Section 6 explores future thoughts for society and the Future Internet.

2.3 Methodology

The SESERV project aims to facilitate discussion and debate between those who study and those who build the Internet. The goal is to increase awareness of socio-economic concerns within the FI community and to help all understand the potential of emerging technologies. The thoughts and opinions from the community have been gained through a variety of sources.

- **Survey of FI Projects**[7]: to understand the interests and perceived importance of societal concerns of the Future Internet community an online survey was conducted with Challenge 1 of which there were 34 responses. The responses from the projects were grouped by Challenge 1 objective to establish common interest within a given area of research. This was used to guide discussion at workshops and to identify areas that require further investigation.

[5] Kalogiros, C., Courcoubetis, C., Stamoulis, G.D., Boniface, M., Meyer, E.T., Bourse, D., Stiller, B. (2011). An Approach to Investigating Socio-economic Tussles Arising from Building the Future Internet. In *2011 Future Internet Assembly*. Springer.

[6] The European Commission (2010-2020) The Digital Agenda http://ec.europa.eu/information_society/digital-agenda/index_en.htm

[7] M Boniface, J B Pickering, E Meyer, C Cobo, A-M Oostveen (2011) Initial SESERV Survey Results (May - 11) Challenge 1 Projects Socio-Economic Priorities http://www.scribd.com/doc/55350692/SESERV-Survey-Results-May11

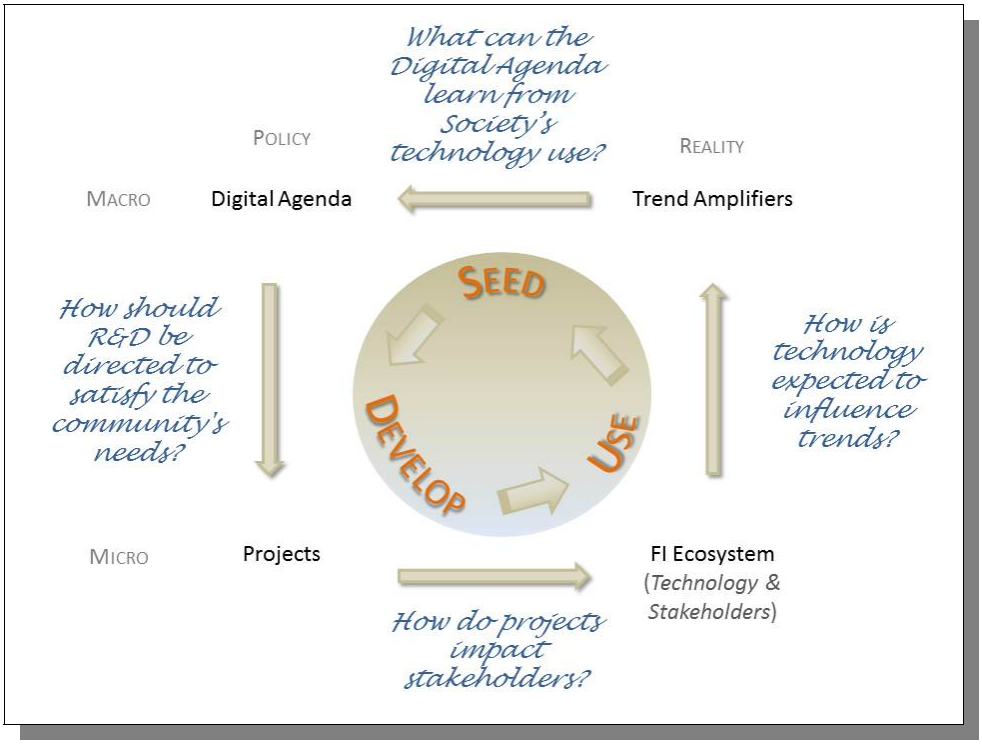


Figure 1: Structure of SESERV's societal coordination activities and report

- **FIA Sessions**[8]: SESERV has organized two FIA sessions during the 1st year of the project on Information as an Economic Good and the Economics of Privacy. Although each session had an economic focus the societal aspects of moving towards qualitative value and privacy rights have direct relevance to this report.
- **SESERV Workshop**[9]: The SESERV workshop "Building the Future Internet: the Social Nature of Technical Choices" brought together interested parties from FP7 projects and academia, including keynote speeches from social scientists and the European Commission (EC). Given its breadth, it may be viewed as a microcosm of the relevant players across societally targeted FI activities. As such, this deliverable draws together the main social themes from this event. The agenda was based on the results of the online survey to identify those specific topics which participants would most like to discuss and revealed some gaps in focus from technologists in respect of the intentions of the Digital Agenda for the projects surveyed. To go into more depth on topics six breakout sessions were organized and specific interviews with project participants conducted.
- **Direct Project Engagement**[10]: A selected set of projects with societal concerns were critically reviewed to identify what technology is being produced and its impact on the FI ecosystem. Risks and opportunities with regard to the Digital Agenda and the Social Impact studies[17] were assessed. A view of the main stakeholders and the value

[8] SESERV D1.1 First Year Report on Conference Session http://www.scribd.com/doc/62317438/D1-1-First-Year-Report-on-Conference-Session
[9] Building the Future Internet: the Social Nature of Technical Choices http://www.seserv.org/fise-conversation/seservworkshopbuildingthefutureinternetthesocialnatureoftechnicalchoices; see also http://www.seserv.org/panel for session summaries and video-casts.
[10] See Appendix I for an analysis of projects

relationships were analysed, along with any specific links between the projects and the views expressed by participants and project partners during the SESERV workshop.

The overall conceptual model for this report is shown in Figure 1. The report considers four key elements and relationships between them:

- **FI Ecosystem**: the stakeholders within the Future Internet and their relationships organized considering value creation, value flows, stakeholder concerns and tussles
- **Societal Priorities**: important real-world themes within society influenced by technology within the FI ecosystem
- **Digital Agenda**: policy initiative from the EC that defines the strategy for ICT research and development targeting future growth and development of Europe.
- **Projects**: projects funded by EC within Challenge 1 to develop Future Internet technologies

The *Macro Level* encompasses both the creation of the overall strategy at the start of the cycle, as well as societal trends in technology adoption, once it is being used. Usage informs, or should inform, strategic direction setting. The *Micro Level* includes technology development (such as the ICT projects funded by the EC) in response to the strategy and policies laid out at the macro level. Technologies are adopted and used within the FI ecosystem by business and society which directly influences societal outcomes.

3 The FI Ecosystem – A Societal Perspective

The Internet cuts across all aspects of our lives, professionally and commercially as well as in our personal and leisure activities. It is important to be online to take advantage of cheaper sales (e.g., economics of scale offered by clouds), in some cases to be allowed to travel (e.g., US immigration now directs visa applicants to an online service), and to keep up with friends and family in remote locations through social networking sites. Moving forward, the Future Internet will be vital in supporting society even more broadly as usage increases beyond simple message exchange and ecommerce to a wide variety of new applications. Given its relevance, then, it is not surprising to see significant global research and development focused on the Internet.

As we move into the future, there are fundamental questions that are being raised. Will, for instance, the infrastructure be sufficient to support projections about increased traffic (see Table 1)? How will users access services, given that mobile devices are becoming ever more powerful? And will all those who want to get online be able to?[11]

Questions of technology, including infrastructure, need to be seen though in the context of the proliferation of social engagement online (e.g., The *Arab Spring*, especially events in Tunisia and Egypt). Social networking activities began as a means to keep in contact with friends and family, but have now become an environment for commercial activity[12] as well

[11] Dutton, W.H., Dopatka, A., Law, G. and Nash, V. (2011) Freedom of connection, freedom of expression: the changing legal and regulatory ecology shaping the Internet. Report for UNESCO.http://www.unesco.org/new/en/communication-and-information/resources/publications-and-communication-materials/publications/full-list/freedom-of-connection-freedom-of-expression-the-changing-legal-and-regulatory-ecology-shaping-the-internet/

[12] The SocIoS Project (2011) D6.5 Legal requirements and ethical issues (see http://www.sociosproject.eu/Downloads/Deliverables/tabid/119/language/en-GB/Default.aspx)

as political engagement[13], and in some cases a forum for the exchange of privately created content[14]. Indeed, social networking site (SNS) participation is already far in excess worldwide than the predicted online population for all 27 EU member states to 2014 (see Table 2).

In the following sections, we consider in some detail the extent of Internet participation, before moving on to examine the FI ecosystem in terms of stakeholders, concerns, challenges and research priorities.

3.1 The Internet and Society

Any report that tries to predict future trends for the Internet or technology paints a picture that is complicated at the very least[15,16,17]. The growth of interconnections between applications and technology has always created, and continues to create, an increasing interdependence between societal development and events. Society and technology are intertwined to a degree that it is sometimes difficult to separate the two conceptually. Technological determinists believe that technology independently causes change in society, while constructivists believe that all technology is socially constructed and only gains power through the meanings attached to it by human actors. Most academic disciplines (including social informatics and science & technology studies) now understand the relationship to be a blend of technological forces and social shaping, but the technological determinist view is still widespread in public use. Thus, the debate continues on whether the FI will be driven by society or technology[18], when in reality it will certainly be a blend of both, and each will encompass many individual factors as well. What is clear is that the Internet has emergent properties that allow certain events to occur irrespective of technological design. For example, consider SNS and the recent Arab Spring[27]. By most accounts, SNS technologies were a key factor allowing the protesters to coordinate and communicate. A technology once used for simple communication between friends, families and colleagues was in this case used to promote certain ideologies, including democracy, freedom of speech and the need for social change. We cannot, however, simply conclude that the Arab Spring was *caused* by technology. The technology probably enabled the events to occur, and almost certainly enhanced the ability of the protesters to succeed in their goals, but we cannot conclude that *without* technology, the events of early 2011 in the Middle East would not have happened at all. They may still have occurred in a different form, or they may have been less successful, but we can't know that for certain. In a recent study on the Social Impact of ICT[17], van Dijk argued that most ICT developments over the last 25 years have not created social trends as much as amplified already existing trends, and that some technological developments (such as the Internet) have been more defining than others. There is every expectation that Future Internet technologies will

[13] The WEGOV Project (2010) D5.1 Scenario definition, advisory board and legal/ethical review http://www.wegov-project.eu/index.php?option=com_processes&task=listDocuments&id=11&s=1&Itemid=14
[14] The TA2 Project (2008) D2.1 Design and Market Insights http://www.ta2-project.eu/deliverables/TA2_D2-1_DesignMarket-insights-final.pdf
[15] http://www.nowandnext.com/PDF/trends_and_technology_timeline_2010.pdf
[16] C Blackman, I Brown, J Cave, S Forge, S Forge, K Guevara, L Srivastava, M Tsuchiya, R Popper (2010) Towards a Future Internet (http://www.internetfutures.eu/)
[17] The European Commission (2010) Study on the Social Impact of ICT (D7.1) http://ec.europa.eu/information_society/eeurope/i2010/docs/eda/social_impact_of_ict.pdf
[18] SESERV Oxford Workshop, June 2011, Debate Will the Design of the Future Internet be driven by Technology or Societal Concerns http://www.seserv.org/panel/conferences-webcasts#debate

continue this role as trend amplifiers which define and enable evolutionary, rather than revolutionary change.

The proliferation of uses and involvement online is significant for Europe, and the rest of the world. In a recent report from the FI3P project we can see how critical the Internet is to Europe. Table 1 summarizes recent data and estimates concerning the penetration of the Internet in Europe[19,20]. Across the 27 member states, just over 65 per cent of the population are online in some guise, a figure predicted to rise to almost three quarters by 2014. The industry itself is worth around 150 thousand million Euros, increasing to about 180 thousand million by 2014. Both in terms of user population as well as market value, the Internet is clearly a significant factor in Europe.

Table 1: Importance of the Internet for the 27 member states of the EU[20]

	2009	2010	2011	2012	2013	2014
Internet users (Million)	301	319	335	350	362	375
Proportion of population online	60.4%	63.9%	66.9%	69.6%	71.9%	74.3%
Value of Internet Industry (€000 M)	€122	€136	€147	€157	€168	€179
Growth	-	11.8%	7.8%	7.0%	6.6%	6.8%

For online communities, Table 2 shows recent membership numbers for some of the biggest SNS's in the West as well as the BRIC nations[21]. Worldwide, *facebook*® is the most pervasive and reports the largest current membership. The BRIC nations, with the exception of India, have large, home-grown sites. It is clear from these figures just how important SNS's have become as a social infrastructure for networking, social capital, empowerment and participation. What is more, as recent events both in the UK[22] and the Middle East[27] have demonstrated, the use of the Internet and social networks for societal change cannot be ignored.

[19] FI3P (2011) Deliverable 2: The European Internet Industry and Market (http://www.fi3p.eu/publications/)
[20] FI3P (2011) Deliverable 2: The European Internet Industry and Market, Appendices http://www.fi3p.eu/assets/pdf/FI3P%20D2%20-%20Appendix%20I-II-III.pdf
[21] India is not included specifically in the table of results; according to the article cited, Indian SNS membership is mainly *facebook*. Home-grown SNS are also common, running alongside the global offerings, though their overall numbers do not match those cited.
[22] Recent rioting and looting following the shooting of Mark Duggan in the UK.

Table 2: Social Networking Site Membership Levels

Social Network Site	2011
MySpace	>125M
Twitter	200M
Facebook	>640M
Ozone (*China*)	480M
VKontakte (*Russia*)	110M
Orkut (*Brazil*)	120M

Source: RIA Novosti 2011[23]

The high incidence of online participation (around 75 per cent by 2014) and significant numbers subscribing to SNS's is especially noteworthy. Online communities of all kinds exist to support leisure and commercial purposes, information sharing and lifelong learning[24,25,26]. The empowerment of individuals to publish quickly to large networked communities means that social use of the Internet goes beyond person-to-person communication. The issues are now concerned with the right of all individuals to seek, receive and impart information and ideas of all kinds through the Internet. The Arab Spring is just one event which suggests that the social uptake of technology extends beyond leisure and commercial uses to political organisation within the community and other societal purposes[22,27].

What is clear is that the Internet is now a medium that facilitates participatory information sharing and collaboration in the creation of content, and that many individuals (but still not the majority) are no longer passive recipients, but also active publishers of information. This characteristic allows individuals to share critical views and to find objective information whilst contributes to the discovery of the truth and progress of society as a whole. The consequence is a changing relationship between the state and the citizen's use of the Internet through legislature and policy actions such as notice-and-takedown regimes, censorship, inequality of Internet access and freedom of speech. Recent reports have examined the impact of policy initiatives such as restriction of Internet content (e.g., arbitrary blocking and filtering, criminalisation of legitimate expression, imposition of intermediary liability), disconnecting users, cyber attacks, privacy protection and the digital divide. The broad conclusion is that freedom of expression is directly linked to freedom of connection and that there should be as little restriction as possible to the flow of information via the Internet, except in a few, exceptional, and limited circumstances prescribed by international human rights law.

[23] http://en.rian.ru/infographics/20110228/162792394.html
[24] Dutton, W.H. (2008) "The Wisdom of Collaborative Network Organisations: capturing the Value of Networked Individuals", Prometheus, 26:3, 211-230
[25] Dutton, W.H. (2010) "Capturing the Value of Networked Individuals: Strategies for Citizen Sourcing", presented at NETworked Organisations, organized by SINTEF, at Kanonhallen, Oslo, Norway, 10 November 2010
[26] Yang, L and Lan, G.Z. (2010) "Internet's impact on expert-citizen interactions in public policymaking – A meta analysis" Government Information Quarterly 27, 431-441
[27] http://www.guardian.co.uk/technology/2011/jul/07/telecomix-arab-spring

3.2 Future Internet Stakeholders

In 2009, the Internet Society defined an Internet Ecosystem[28]. The stakeholders originated from a traditional infrastructure perspective, with the main portion of the supporting document describing the responsibilities of the various standardisation bodies involved in what they refer to as *Open Standards Development* and *Naming and Addressing with freely accessible processes for Policy Development.* However, in recent years, the rapid convergence of technologies has increased the scope of stakeholder engagement with the Internet way beyond what was originally envisaged and described by the Internet Society. The European Future Internet initiative has been at the forefront of such developments both within the core ICT programme and the FI-PPP initiative[29]. The former is primarily focused on B2C scenarios where the latter specifically targets sectors of societal importance in urban environments such as energy, environment, agriculture, logistics, transport and content.

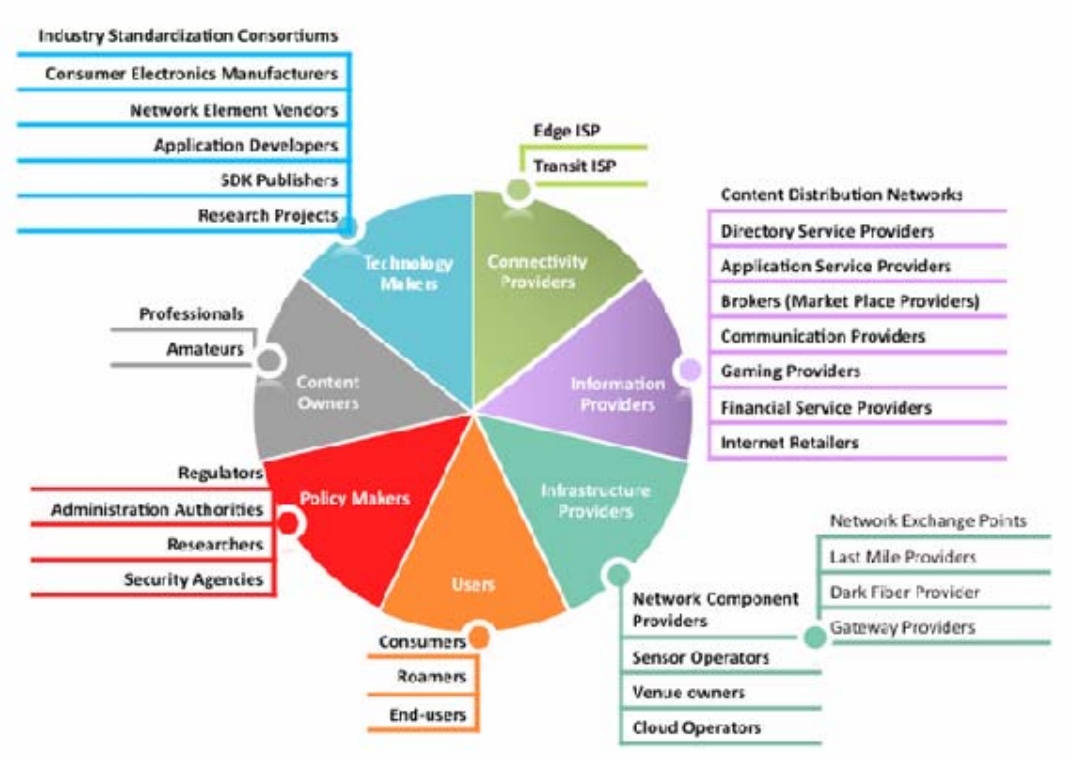


Figure 2: The Future Internet Ecosystem

A number of different models have been proposed for who the stakeholders might be within a Future Internet ecosystem. SESERV deliverable D2.1 “First Report on Economic Future Internet Coordination Activities” has defined a possible FI ecosystem[30]. The ecosystem was created by completing a tussle analysis on a set of Challenge 1 projects. The proposed ecosystem provides a static classification of stakeholders whose dynamic characteristics will be explored in more detail during year 2 of the SESERV project. We see in this new model a significant increase in the diversity of roles, an increased emphasis on users in addition to previous infrastructure and a blurring of roles between

[28] The Internet Society (2010) The Internet Ecosystem http://www.isoc.org/pubpolpillar/docs/internetmodel.pdf
[29] http://www.fi-ppp.eu/
[30] SESERV D2.1 “First Report on Economic Future Internet Coordination Activities”

major market players. The concerns of the Internet have moved from structures purely targeting transit and delivery of data to socio-economic structures supporting exchange of information and knowledge according to the values of individuals and communities.

This view is confirmed by the FI3P[31] project which has defined the Internet actors in terms of two domains: the Internet IT/Networks Industry and the emerging Web Ecosystem (Figure 3). The model considers not only the providers of the infrastructure (the bottom layers), but also those providing services on that infrastructure and the business and private consumers making use of those services. From the FI3P perspective, the traditional actors in the Internet space are the infrastructure providers. These need to be contrasted with the emerging actors they see: namely, the application service providers and the consumers of those services. The focus here is therefore very much on the exploitation of the network infrastructure by both providers and consumers.

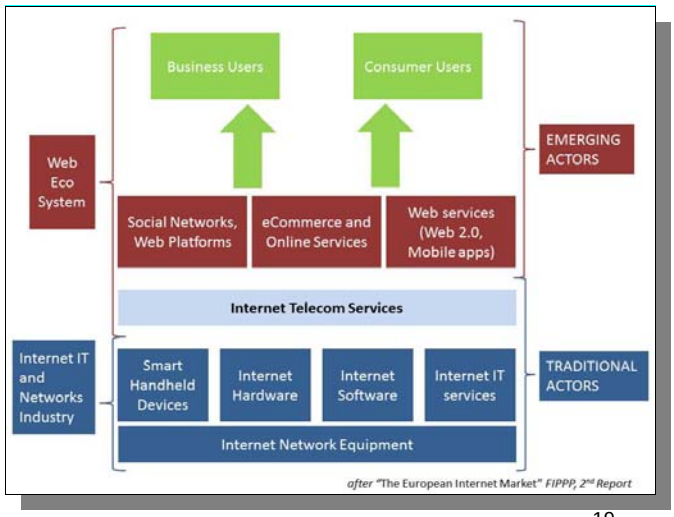


Figure 3: Internet Actors from the FI3P[19]

Of course, no single research project can address all stakeholders; even the FI-PPP has its limits in terms of application areas and technical scope. Some are specific (e.g., social networking for eGovernment) and others targeting key stakeholders supporting value creation within the ecosystem have a broader impact (e.g., infrastructure providers). Examining a set of projects we can see how various stakeholders concerns are addressed (See Table 3).

Table 3: Projects and Stakeholders Interests

Project	**LAWA**	**SENSEI**	**Smart Santander**	**Social nets**	**SocIoS**	**TA2**	**WeGOV**
Policy Makers							
Investor	Commission		Administration Authorities; Commission	Commission			

[31] FI-PPP and FI3P are used interchangeably in this document.

Project	LAWA	SENSEI	Smart Santander	Social nets	SocIoS	TA2	WeGOV
Policy Makers		Regulators	Administration Authorities			Regulators	Legislature
Provider							
Infrastructure Providers		Wireless Providers (purpose = Environment); **Project** (purpose = Environment; Access)	Infra. Providers (purpose = Environment); **Project** (purpose = Access)	SNS (purpose = Environment);	Open Social (purpose = Technology)	Infra. Providers (purpose = Environment)	Cloud providers (purpose = Environment)
Information Providers	**Project** (purpose =ALL)	Service Providers (*purpose = Access*); Pervasive technologies (*purpose = Technology*)	Internet Developers (*purpose = Technology*); Pervasive technologies (*purpose = Technology*); Service Providers (*purpose = Access*)	Service developers (purpose = Technology) **Project** (purpose = Access);	Developers (purpose = Technology) 3rd Party Services (purpose = Technology) SNS (purpose = Environment) **Project** (purpose = Access)	Technologists (purpose = Technology) **Project** (purpose = Access);	SNS (purpose = Environment; =Access); **Project** (purpose = Access; = Technology)
Content Owners	Content Providers (function =Information)			Online Communities (*function =Information*)	Online Communities (function =Information; =Personal)	Families (purpose = Entertainment; =Personal)	Project (purpose =Information; =Personal)
Consumer							
Research Projects	Internet Researcher; Research Communities *(rôle = Scientist*)		Internet Researchers (*rôle =ALL*)	Sociologists (*rôle =Scientist*)	Research bodies (*rôle = Commercial*)	Technologists (*rôle =Scientist*)	End-Users (rôle = Government)
Users		End Users (rôle =Participant)	End Users (rôle =Participant)	Online Communities (*rôle= Participant*)		Families (rôle =Participant)	Citizens (rôle =Participant)

3.3 Societal Concerns and Challenges

There are many societal concerns that emerge as a consequence of FI research and development within projects. Defining a set of concerns that relate directly to the FI ecosystem, rather than more general societal concepts, is essential for engaging Challenge 1 projects in discussion and debate. Recent reports, *Social Impact of ICT*

Studies[17] and *Towards a Future Internet*[32], were used to identify key societal concerns (via content analysis of both documents) for the FI that raise significant technical, commercial and regulatory challenges:

- Regulation of the Internet
- Privacy and data protection, including user data, file-sharing control, selling of personal information, etc.
- Online Identity, including anonymity, digital presence, rights to delete information, etc.
- Security of communications, including legal implications
- Cloud computing, including the risks and benefits of virtual access to information, etc
- Green Internet issues, including reducing the carbon footprint of the ICT sector, e-waste, etc
- Content regulation, including copyright, licences, open access, etc
- E-democracy, including transparency, open government data, empowered citizenship, services to citizens, etc
- Digital citizenship, including individual and corporate rights and responsibilities, etc
- Digital inclusion, including access and use of Internet by vulnerable populations, etc
- Trust, including risk drivers, actors at risk, risk management, etc
- Online communities, including social networks, virtual relationships, etc
- Internet of things, and the connections between people and devices
- Relationships between consumers and suppliers online
- Distributed knowledge production, including e-science, e-learning, etc
- Cybercrime and Cyberlaw, including phishing, cracking, cyberterrorism, etc

These concerns were reduced to a small set of topics related to the interests of Challenge 1 projects[33]. The following sections present the outcomes of discussions with community members. Each of the following sections was drawn from conversations among technology developers and socio-economic experts, primarily facilitated during the breakout sessions and interviews at the Oxford SESERV workshop held in June 2011. The boxed quotations summarize salient points on each topic that arose from these breakout sessions.

3.3.1 Risk Management - Security of Communications

Is there really a difference between “security”, “online identity” and “privacy”? Security of communications is not about privacy or data protection and management in the face of any new invasion of privacy, nor about forms of identity and anonymity in the context of digital presence. Instead, this is about managing the risks to business efficiency and

[32] C Blackman, I Brown, J Cave, S Forge, S Forge, K Guevara, L Srivastava, M Tsuchiya, R Popper (2010) Towards a Future Internet (http://www.internetfutures.eu/)

[33] M Boniface, J B Pickering, E Meyer, C Cobo, A-M Oostveen (2011) Initial SESERV Survey Results (May - 11) Challenge 1 Projects Socio-Economic Priorities http://www.scribd.com/doc/55350692/SESERV-Survey-Results-May11

effectiveness, to both critical and non-critical infrastructures, to financial stability, and to personal security and trust. Security in this context, therefore, is about risk management.

Cloud computing is a fundamental component within the FI Ecosystem. While cloud computing could provide access to great resources, clouds raise concerns about the risks they could put users and societies under. Clouds provide their customers with instant access to large-scale data storage and processing facilities. But what type of risks do clouds pose to society, to individuals and to businesses? Consider, for instance, just two questions:

- What if cloud providers or their customers were malicious? For instance, because they have been compromised by criminals, they are criminals or they don't care about some potential threats?
- What are the possible threats? DDoS attack using a public cloud (possibly procured using stolen credit card details), the mobile (in IP space) casino, child pornography site, phishing site, etc. For instance, someone renting a cloud with a stolen credit card, or using a cloud to create a virtual casino to evade taxation. Can pornography or phishing sites be moved around using clouds?

Another example of potential security risks within the FI Ecosystem is sensor networks. They can be used in services that expand from traffic management and health warnings to advice on the best routes for cyclists. Reusable sensor networks can enable applications such as pollution monitoring and environmental management, public safety and emergency response management, traffic monitoring and optimization, etc. However, what if a malicious agent could spoof the sensor data? What are the possible threats? For example, a farmer corrupts humidity sensors to increase the irrigation of his fields, retail hackers fake a traffic jam to divert customers from a rival store, a terrorist corrupts humidity sensors to reduce irrigation and kill crops. These are all security threats (as opposed to privacy or identity issues). So how can we block these potential abuses?

For cloud computing there are significant non-technical questions, issues and challenges. Who is (or should be) responsible for meeting the security threats of clouds? The operator of the cloud or the sensor network? The developer of applications that access and use them? The customer for those applications? The bystanders affected by them (e.g., the victims)? Social or governmental agents (e.g., police, social networks)?

> *"Risk-management with respect to common infrastructures used for the delivery of services, i.e. clouds and sensor networks. Distribution of control, responsibility and liability in infrastructures. Access to risk expertise. Lack of capacity to assess risks"*

And in such cases, how can responsibility be attributed? Do you impose responsibility by regulation, or self-regulation or market forces? There is no easy way. There are major concerns of what could happen if you impose responsibility to protect from security risks. One extreme scenario could be that the cloud provider becomes the key party responsible for the cloud. This could have serious implications for the degree of freedom users could have. In contrast, the implications of not having any regulation could lead to risks of outlawing part of the innovation. Will the responsibility and potential liability deter anyone from offering innovative Future Internet services? Will the potential impact lead society to outlaw them?

There are no easy and general solutions. But starting with getting all parties involved together and bringing them to understand the risks involved is the first step.

The first question is: ***who should be responsible for providing countermeasures in case the clouds are being misused?***

- Option 1 (users): Consider a case wherein attackers succeed in convincing a population of users to install malware; the attack in such cases can be scaled up very quickly. Does that mean people must have the equivalent of a driving licence before using a cloud? If we needed a licence for owning a PC, that would have stopped the PC market, but now what do we do with owning a cloud given the risks involved? User ability can vary, and there could be so many ways into a cloud or a sensor network. Most of the protective measures would simply be to inform users of the precautions they should be taking. But because there are so many ways, some attacks would always work.
- Option 2 (Infrastructure providers): Another scenario is to ask infrastructure providers isolate the cloud from suspected users. If the cloud provider has a hacker or password cracker, can the cloud provider take responsibility to prevent the attack from happening? If for instance, one user is suddenly using the cloud very strangely and it turns out a hacker is using stolen credit details. The cloud provider, in principle, could detect abnormality; but should they be responsible for protecting the user? The cloud provider has to make that choice for the user.

Another important question is: **does the cloud provider want to have any responsibility for what they do?**

The issue of variations of legal measures between countries is of particular importance. In Italy, for instance, the law puts liability on the service provider of YouTube and Google. You would have the same problem with clouds. If the service providers are not using measures in line with the laws of the countries they are operating in, this may discourage them working together in that country. At the moment no cloud providers explicitly accept responsibility.

It is difficult to discuss security risks appropriately without a scenario. Perhaps we should start with an assumption that sensors have been mis-configured on purpose, then we can deduce a number of consequences and scenarios. Technically it is possible to detect a cloud abnormality but it is not that straightforward. The outbound and inbound traffic may have statistical information that can ensure that the user is not behaving differently compared with the past. In such a case, it would be possible for cloud providers to use the 'credit limit' of the user as a way to stop any abnormal behaviour. However, it would not be possible to detect the scale (except for password cracking). But what if users do not have much history with the provider? Indeed, typically, if someone wanted to do something wrong with the cloud, they would not be planning to stay for long - they would quickly do something to the system, then move out. So how can we address these behavioural differences technically?

The issue of ***protecting the data*** is another challenge. When we look at the security challenges, we are – by default – getting into the problem of data protection. If we cannot protect the data how can we guarantee that the services can be protected? Moreover, the infrastructure provider might have a mechanism for detecting a micro hotspot, to detect when something is "hot" (e.g., a data fusion system); but then someone could use the data from this network to advise a GP on what to expect at their surgery the following morning.

It brings a new challenge, namely how the data can impact others - or conversely - how sensor corruption risks should be managed.

Security can be addressed via technical requirements, but the more difficult, emerging challenges are socio-economic: how does it affect the obligations of those who didn't expect to be supporting these services? Example: in India, there are sensing networks that measure humidity in fields. If you were a farmer would you be able to use this and would it increase your crops? It really depends on whether you will use it for agriculture, finance, or other purposes. And what if someone goes and changes something? How will it affect the farmer's business? One suggested solution is having multiple sensors to avoid misinterpretation via a single sensor (e.g., if one gets attacked, the effect will be cancelled out over the total number). But the economic implication is important to consider. Having one hundred sensors is more costly than having just one. We also have to have a number of different monitoring points.

Access risk expertise and managing risk are essential. The cloud provider has a team of security analysts or information security analysts, and large corporations employ large defence companies. You have to have a team of legal, security and technical experts. If you are developing the technology, you ought to be the expert already. However, not everyone has access to risk experts or to cope with security threats. Most medium and small scale companies cannot afford to hire technical risk analysts (on top of lawyers and other experts). Similarly, home users just trust the information they are given. These users would be unlikely to hire a technical expert to analyze the risk situation at home. What should they do? Should they just trust the information they get?

Another issue is the ***lack of manpower*** to handle all monitored detections. The example of Swiss banks and money laundering detection was given as similar to cloud fraud detection. The bank created a system for detecting potential money laundering fraud. Within the first few days, thousands of cases were detected by the system but nobody had the resource to look at them. The speed and volume of data can cause a challenge to manage.

The issue of providing technical advice as part of the service provision of clouds is also important. Swisscom offered a security package for a fee to its customers, to which many people subscribed. But users ended up getting nothing but software updates to ensure security. For some kinds of stakeholder, it might be enough just to have an add-on security feature. But for bigger operations like companies or universities, getting technical expertise from the service provider would be difficult.

There are various strategies to bridge the gap and provide potential solutions:

- Policy makers: change the regulatory framework: One possible strategy is to allow policy makers to anticipate what could go wrong and analyze frameworks of detection. This is the same as bank systems detecting money laundering. It would only work if you have a mechanism for anomaly detection. But there are certain issues worth considering:
    - Where there is a risk, could one impose an obligation on (say) infrastructure providers – similar to Anti-Money Laundering regulations?
        - The problem with legislation as a solution is that cloud providers might not operate in the specific country, and different countries have different laws. Also even though they have to comply with existing EU legislation on handling storage, privacy etc, the nature of the cloud brings new risks.

  - Many SMEs are thinking to move their regular ICT needs into a cloud. For a smaller company it might be better NOT to have many policies and regulations. Often regulations lag some five years behind technology invention.
  - You could regulate, but on the other hand, you have got to deal with the possibility that it might be going on all the time. And you should be ready for the risks, and that this could create a huge amount of work.
  - You can make service providers manage the risks. Customers need to trust the infrastructure provider, but if users feel they are closely monitored, they might not feel comfortable with the service. We have to be careful about what can or can be detected.
- We need to keep up with the technical developments (and monitoring it) but not be ahead of it. And we need to avoid creating new problems or unexpected side effects by technology. Like in the case of the Swiss bank attempt to detect money laundering cases, the system showed thousands of small cases that they did not have the capacity to monitor.

- Security Agencies: or forums like the Cloud Security Alliance[34]
  - One solution could be to engage technical and legal analysts to understand risks and assess new risks. We can only address risks within the current framework – assessing new risks is always harder. Also, not everyone has access to risk experts. You need more than just a lawyer, you also need someone who can understand the technical aspect of it.
  - Technical assistance from service providers could be another solution, but would it be enough? Currently, the most that could be provided is a set of best practices and guidelines to be shared with users.
- Market Forces: will customers reject services that are bad for society?
  - One possible solution would be to leave the security to the market: customers may not use services that they find too risky. But the *laissez-faire* of a total free market style, like what happened with the financial crisis, cannot be enough to manage security risks. There should be some regulation and rules informing the market. One simple approach could be to force cloud service providers to publish statistics about the health of their activities and their monthly attacks. On that basis, it could be checked by a government authority or a third party.
    - Would providers publish data on this (or could they be forced to)? Incentives could also be given to service providers to publish health reports periodically.
    - But since security is very sensitive information, service providers might not be willing to reveal those data so as not to lose customers (in much the same way as banks would hide cases of money laundering through their institution). We therefore need metrics for comparison of 'trustworthiness' and of the anti-risk health. They must be publically available to allow users to compare across service providers.
    - Some auditing standards must also be established, to ensure that what service providers publish is credible.

[34] *https://cloud**security**alliance.org*

- It is also possible to allow a community of users – who are not the police or regulators or individual customers but networks with common interests - to help work together to monitor services and improve the cloud systems. This is through enabling platforms for peer to peer interaction.

"Erosion of choice and control due to increasing asymmetry between consumers and mega providers. Unauthorised reuse of personal data. Complexity of decision making when accessing services. Fundamental Human Rights"

- Are there any risk analysis models that cloud operators use? Service providers probably have some but they must also look at the integrity of their network – and what it can do. You can analyze their risks for them, but as soon as you do that, you expand your scope and add to your cost of analysis.

3.3.2 Privacy

As the Internet becomes more integral to the way we live our daily lives, end users are becoming increasingly aware of the dangers of making too much information available publicly. People's careers and personal lives can be severely affected if they do not consider carefully what information (including multimedia – photos, videos etc.) they make available about themselves in cyberspace. Certainly there is a trend towards increased privacy awareness, although attitudes towards privacy are changing significantly – for many, the level of privacy concern is decreasing. This raises some interesting questions about the role of privacy-enhancing technologies and privacy-related research in the future.

The low-point for privacy was reached in the first decade of the millennium. The enthusiasm of citizens for Internet applications (Web search, Web publishing, social networking, etc), combined with a neglect for basic security by the application operators led to a free for all. The abuses at this point fell into two main classes:

- Citizens found that information about their activities in one context (e.g., social life) was publicly accessible and could be used against them in another (e.g., professional life);
- Citizens found that even information that was supposedly confidential (e.g., between themselves and the service provider) or restricted (e.g., to a select group of friends) could be viewed and passed on by others.

Uncovering supposedly confidential data involved some modest effort, so typically the victims of confidential data disclosure were persons of some notoriety. For most users, the main concern was the extent to which they were making information public. People are now addressing this concern by allowing less of their content to be published for anyone to see. This improvement in general awareness will make Future Internet applications safer (e.g., customers and regulators will demand that smart grids and location-aware services protect user privacy).

However, while the low point may have been passed, privacy is still heavily compromised by a lack of deeper awareness as much as by technical or cost issues. Users supply huge amounts of personal information to service providers with every post, query or click in

applications like Google Search, facebook, Twitter. The providers of these services exploit this content in a wide variety of ways:

- to attract a larger audience share, many of whom will themselves become users;
- to classify users based on their personal data (profiles and traces), allowing personal characteristics to be extracted and used to 'improve' the service;
- to classify and index data (including personal data relating to other users), allowing the service to be further enhanced;
- to provide information to other organizations including businesses and governments, for payment and/or to meet legal obligations.

The most successful service providers are now among the largest and most profitable businesses on the planet. Yet they typically accept no responsibility for user-generated content, leaving the users to bear any consequent liabilities[35]. Users can publish sensitive, sometimes scandalous information about third parties or each other, which is propagated freely by the service provider, often attracting large audiences. The victims have no protection and very limited recourse. They can ask the service provider to remove the offending content (after the damage is done), or they can sue the user who posted it (if the service provider reveals their real identity, and that user is under a jurisdiction to which the victim has access).

Citizens do benefit from this exchange, because they can use search technology, social networks and so forth without charge. But the relationship between citizens and service providers is highly asymmetric, and the resulting loss of privacy for users and bystanders is profound.

The trends are towards an increase in asymmetry as service providers improve their exploitation and find new opportunities to capture personal data from their users. Personal data is increasingly available to the service provider and (if it serves their purpose) other users, commercial customers and government agencies. Freedom of choice is being eroded as the services provided (Web searches, online shopping, etc) are increasingly filtered based on the provider's analysis of user preferences. The risks from widespread disclosure should the provider be hacked or forced by government agencies to release information are growing ever greater. European privacy regulations provide little protection due to technical and jurisdictional limitations and, if anything, just make it harder for European service providers to innovate and compete in a global market.

Privacy clearly goes hand-in-hand with issues of security and trust. It is reasonable, therefore, to expect appropriate technical and procedural protection in support of users once they are online. To some degree, users may have unrealistic and exaggerated expectations of such technical provision for privacy. However, it is equally true that users are able themselves to make appropriate judgement about suitable protection and data management. It is probably not always appropriate or necessary for the blanket application of regulation. Instead, viewing how users behave and *wish* to behave may help determine what is really required.

In terms of potential solutions and strategies researchers need to be working towards the following vision:

[35] Though this is not always the case. Italian law puts the onus on the service provider; cf. Section 3.3.1, p23.

- Compliance with European privacy regulations by European service providers is highly valued by European (and other) citizens. European notions of privacy and associated regulation provide opportunities for European service providers, rather than holding them back.
- Users retain control over their data, not merely telling the service provider how public to make it, but also controlling access by the service provider itself. The most confidential data is held on user-controlled devices on the cloud edge. Service providers can access it in specific ways, using secure computation to minimize their access to the raw data.
- The relationship between European citizens and service providers is a balanced one. In particular, service providers cannot derive business (not limited to financial) benefit from user-generated and personal data capture and processing, yet avoid any responsibility for the consequences.
- Victims of malicious publication have far more options than before. The primary beneficiary (the service provider) has a greater level of responsibility. The source of malicious data is accountable even if not traceable, and subject to community sanctions such as temporary loss of service. The malicious publication can also be deleted from the Future Internet, even if propagated to other service providers.

> *"Diverging definitions of identity. Society conceives stable identity but online identify is inherently dynamic. Relationship between online identity and data."*

- The European concept of privacy has evolved to provide a more robust framework of rights and obligations. This provides more effective protection of human rights, yet it also supports rather than inhibits technical and commercial innovation by compliant (including all European) service providers.

3.3.3 Online Identity

Online identify has moved beyond just the technologies, devices, applications or technical challenges. The concern today has switched to the more fundamental question of how identity is to be understood within the context of (user) interactions in different socio-technical environments. Online identity is closely and inextricably related to issues and relationships between data, privacy and rights (including, though not limited to, digital rights).

Rather than being closely related to specific technologies, devices or applications, questions of identity are here framed as a series of interactions in multiplex socio-technical systems. In an online context, identity as a theoretical construct is closely related to questions of data, privacy and rights (including, but not limited to digital rights). It thus becomes necessary to address and determine the relationships between data (all data/private data) and identity.

Identity is not easy to define, and current definitions are diverging. There is a need for the development of common definitions, and vocabularies enabling a multidisciplinary discussion of identity. Society conceives identity as stable: identity in terms such as surname and passport, etc. is conceived as being stable predominantly by society/policy-

makers and in societal contexts. Yet, in scholarly discourses and research on identity, identity is often characterised as inherently dynamic. In addition, individuals might very well experience their identity/-ies as dynamic. This clash between the two opposing stances is currently not sufficiently addressed.

A number of socio-technical challenges exist:

- Developing tools for managing online identity, including multi-scale filtering of content is important. End-users could benefit from having a set of tools assisting the management of their online identities across platforms. As applications are increasingly bridged and interwoven, users need assistance in understanding the implications of this on the sharing of their data, and identity/-ies. Designing tools that enable multi-scale filtering of content by users, e.g., by giving more control of which date/information is accessible to whom, is an immediate challenge to be addressed.
- Acknowledging and managing identifying features of large-scale data. In an online/networked environment, users leave digital footprints behind. These footprints are data that can be harnessed or misused by third parties. In addition hereto, more sophisticated methods for analysing large-scale data from, e.g., achieved system logs, mobile phone usage, and online actions by users, make is possible to identify individuals based on their preferences, patterns and social networks. This places an increased onus on developers, legislators, third parties and researchers to address and communicate the degree to which data reveal identity. Moreover, it poses the challenge of finding ways to anonymize individuals (data and identity).
- Determining acceptable levels of anonymity online, and designing systems supporting these. As anonymity cannot really be guaranteed online currently, single users can (with some effort) always be identified. It is important to determine which levels of anonymity should be allowed under which circumstances and contexts. Also, there is a need to address whether anonymity should form part of a more general set of digital rights. In extension of this, a challenge is to develop features that will allow for increasing levels of transparency for end-users. Individual users should be made aware of the level of, or lack of, anonymity given that systems allow for.

There are various strategies to bridge the gap and provide potential solutions:

- Facilitating further formal and informal digital literacy education, which can equip users with more sophisticated tools for managing and understanding identity in online and hybrid contexts.
- Develop initiatives that raise awareness of issues related to identity management in the 21st century.
- Fund interdisciplinary research that can inform discussions on what constitutes identity, and how these can be translated into socio-technical system features.

"Tension between public perceptions and the potential of the technology. Need to engage with ethics and privacy experts."

3.3.4 Internet of Things (IoT)

There is a general issue about the definition of IoT technologies. Basically, existing technology is undergoing constant update and enhancement with onboard “intelligence”. At the very least, the IoT can be thought of as including all manner of mobile devices, including telephones, PDAs and sensors, enabling the creation and indexing of intelligent and exhaustive databases. The key factor for IoT technologies is the enablement of seamless interaction between different systems; IoT technologies are bringing data together to create new services.

The IoT has so much promise in terms of taking online technology out to end users as well as the more traditional aspect of sensors which might automate the surveillance and management of the more mundane aspects of life (self-regulating food ordering on the base of fridge monitoring; automated homes; and so forth). But such social benefits may be outweighed if issues around trust are not resolved. Trust in this context though extends beyond specific concerns on security and data protection; there is now a definite interest in involving users in the design and development of ethically-based applications.

The barriers for the adoption of IoT within the FI ecosystem have been identified as:

- Too abstract definitions: Current definitions are hard to grasp. They are too academic and do not focus enough on design/application. This is partly due to the lack of interaction between the actors of these two domains.
- Lack of vocabulary for multi-device interaction: Multi-device IoT interaction does not have a well-developed vocabulary, and it is therefore difficult to facilitate efficient and effective IoT design discussions. Currently, design development is characterised by 'doing' rather than by reflexivity and design discussions.
- General public perceives IoT as Big Brother enforcement: ‘Smart’ applications tend to be received with scepticism by the general public. One example is the ‘smart’ bins in London that were provided with sensors[36]. These were quickly coined ‘spy’-bins.
- Technologies framed as having autonomous forces: In popular discourses, technologies are often being described as independent and intelligent agents acting autonomously; and people as being ‘affected’ passively. Changing this attitude and the underlying technologically deterministic view, would help to inform design better.
- EU's Digital Agenda's influence on IoT innovation/design: The Digital Agenda enforces a certain amount of transparency and privacy for IoT application end-users. For designers and IoT business developers, however, it can be experienced as restricting for new business plans and technology designs. It also affects the global competitiveness.

The socio-economic challenges for IoT include:

- Moving beyond IoT for domestic uses: IoT technologies are predominantly designed for domestic purposes; e.g., the interactive ‘intelligent’ Internet fridge. There is a lack of design and creativity in the domain of IoT. New applications should be implemented in existing infrastructures to make environments more intelligent; e.g., transport systems; health applications.

[36] http://www.thisislondon.co.uk/news/article-23409377-smart-wheelie-bins-to-charge-for-waste.do

- Making multiplex data compatible: The uptake and uses of new technologies in general generates vast amounts of data. Individual systems, however, are not able to harness the data because there is no common agreement on what to do with it. There needs to be an ‘intermediate’ level of technology, to help understand data on individual system levels. The challenge is to design tools that can harness data that is being generated independent of the tool itself.
- Determining boundaries between public and private data: IoT technologies are blurring the boundaries between public and private data. One example is the ‘passive’ monitoring of mobile phones: Walking around with mobile phones switched on, users can be tracked at all times. There is a need for addressing ethical issues around such data. Where are the boundaries between, e.g., public and private spaces, or public spaces and consumer goods?
- Ensuring transparency for end-users: There is a need for ensuring transparency on data usages by corporate entities. Clear statements of advantages and disadvantages (e.g., spam risks) of technologies/services are needed. Users/consumers should be presented with different levels of ‘sign-off’ options.
- Balancing privacy concerns: While privacy is an obvious concern for IoT applications, it is necessary to develop an approach that does not result in moral panic. To that end, it is important to clearly communicate to end-users the implications of using Internet of Things technologies.
- Enforcing the right to digital choice: It is vital to provide opportunities for 'offline' access to services for users who do not use certain technologies; whether this is due to digital choice, or lack of access to certain technologies. ‘Opting out’ currently penalizes people, which should not be the case.
- Developing back-up mechanisms for large-scale system failures/attacks: A major challenge relates to developing security measures for potential catastrophic failures of technologies that would affect individuals, businesses, governments, etc. An example would be a cut-off from the Internet. There is a need for developing adequate offline back-up mechanisms.
- Acknowledging and addressing the possibility of unintended results: consequences of IoT based Socio-technical designs and applications might have unintended outcomes. An example from the health sector: Some elderly people have sensors implemented in their homes, measuring levels of moisture. While such sensors can help alert carers, they might also result in new practices, in which human expertise is replaced by automated sensor-network data analysis. There is a need for ways of assessing and analysing unintended design outcomes of IoT technologies affecting the social world.

There are various strategies to bridge the gap and provide potential solutions:

- Facilitating collaboration between privacy research and engineers. Research in the two domains seems highly disconnected, despite the obvious parallels. These sources of expertise should be brought together for the development of IoT.
- Integrating ethical dimensions as core component of discussions on IoT-'design potentials'.
- Ensuring that policy-makers set up frameworks for connecting designers and users; and help raise awareness.

"Service providers are dictating how communities interact and what happens to their data. Communities want to control and define how to maintain community health."

- Inviting users to play a role in the design of technologies; e.g., by means of market research.
- Funding further ethnographical research on ICT usage in everyday life that can inform design choices.
- Bringing ethics and privacy experts into early stages of design development phases.

3.3.5 Online Communities

Two-thirds of the world's Internet population now visits an online community or blogging site and the sector now accounts for almost 10% of all Internet time. A quarter of a million users sign up to social networking sites every day worldwide and a third of those who have a profile on a social network update it daily. Online communities centre on how users interact with and exploit the range of social networking applications (e.g., government, leisure and work).

The goal to increase participation and maintain healthiness of online communities through the use of popular social networking sites is common in most social networks. A critical success factor (i.e. participation) for social networking providers is to maximise activity, which is largely achieved irrespective of the purpose of the communication between individuals. However, the goal to comply with data protection legislation is also equally valid and as well as necessary is certainly a strict requirement for European providers. Legal compliance requires providers to accept responsibilities (in respect to purpose) and individuals need to take certain actions (e.g., consent). So here lies the contradiction. Privacy compliance, often declared as a way to increase trust, and hence participation, in effect impedes activity and actually acts as an inhibiter to participation. In reality, individuals use social networking sites because their perception of risk is considered low enough for participation. It is the perception of and appetite for risk that dictate levels of participation, irrespective of associated regulation.

This leads to an interesting challenge for European service providers and research projects: How to strike the balance between participation and privacy considering desires to monitor and mine data without violating a citizen's right to privacy? Architectures that facilitate communication between individuals regardless of purpose have been important innovators in the Internet. It is a principle that has contributed to the explosion of Internet use (the end-point principle) and it is improbable that the successful paradigms of the last decade, social networking and clouds, would have prospered if they had considered compliance to the European regulatory environment. Each new paradigm has focused on promoting the benefits of solutions and opted for weak privacy positions. The try-it-and-observe approach has allowed for a privacy balance to evolve over time as participants explored their preferences rather than having them analysed in advance by security experts. Social networking has in fact been a large experiment in people's appetite for privacy.

New key technologies relating to online communities can be understood in the context of the uptake of social technologies such as micro-blogging applications and social network

sites: An application like Path (for iPhone), for example, introduces the idea of limited friendship networks based on the Dunbar[37] number. Thus, this application is about enabling users to better control what information is shared with online social networks. Other key new technologies include the live synchronization of social networking content to multiple networks, in particular user profiles.

Online Communities highlight the basic dichotomy: is it technology or society which will shape the ICT future? The answer is clearly that for now at least there is a real need to back off from technology for technology's sake and begin to take seriously *how* communities are formed and *what* they do online. This would not only move the focus towards society and societal behaviours away from technology, but more importantly would require appropriately skilled cross-disciplinary researchers who would need to examine and explain what appears to be happening in such communities. Participation and privacy are critical success factors that underpin healthy and vibrant online communities. It is essential that Future Internet researchers understand the complexities of participation and privacy in the design of systems to ensure that technologies are socially, ethically and legally acceptable.

The socio-economic challenges for online communities include:

- Developing technologies to support community 'health': With increased participation in online communities there is a need for such support, e.g., growth, structure and maintenance.
- Enabling the linking of systems while maintaining user control and user-centricity: User-centric platform-bridging applications with transparent filtering options should be developed for synchronization of content across platforms and networks. The key challenge being that users should be able to manage and control their information sharing easily with the online communities they are part of.
- Allowing for new communities/structures to drive development: Technologies are not the only drivers of development for online communities; new types of communities could be emerging to shape new technologies, just as different community structures may be required for sharing, or co-creating content. There is a need to balance bottom-up and bottom-down technology development.
- Facilitating better tools for managing online communities: A key challenge is equipping users with tools for managing and creating smaller community hubs mirroring the theoretical cognitive limit for social relationships (c.f. Dunbar's number[37]). Simultaneously, it is important to raise awareness of the limitations and strengths of smaller online communities (e.g., less information accessible). In particular, privacy is a massive concern when sharing information and publishing content online, and increased numbers of smaller online communities might therefore become a way of handling privacy issues.
- Defining a normative framework for technology use: There is a need to define a normative framework for technology use, which might include strategies for managing different contexts.

[37] The *Dunbar number* was proposed by Robin Dunbar as a limit on the number of people we are able to maintain active social relationships with at any one time (see http://www.sciencedirect.com/science/article/pii/004724849290081J).

- Balancing the right "to be forgotten" in the digital sphere: Informed and balanced discussions on the right to be forgotten (have online content permanently deleted) in the digital sphere should be facilitated. This right should not necessarily come to include acts in the public sphere. For example, it might not be right to allow actors/entities having committed crimes against humanity.
- Developing a research tool box for understanding online communities: Moral philosophers and social scientists need a toolbox enabling them to examine and assess online communities better.
- Enabling creative uses of applications to influence system development: Users make innovative and creative use of systems and applications. A future challenge is to facilitate structures for translating and feeding the creativity of users into the system in order to improve and develop it further.

There are various strategies to bridge the gap and provide potential solutions:

"Little common understanding of what clouds are. Europe is slow to embrace the full potential of cloud computing, focusing more on concerns rather than benefits. Playing catch up with regard to business models and regulatory frameworks"

- Examine the frequency and need for multi-disciplinary meetings and conferences, and possibly fund a larger number of multi-disciplinary research centres and departments.
- Delivering further media literacy education to help solve problems related to privacy.
- Initiate research that can generate knowledge on 'behind the scenes'-processes of socio-technical systems, and user motivation.
- Develop regulatory frameworks that are consistent and guarantee anonymity (conditionally or dependent on domain, e.g., if wanting to talk about politically sensitive topics).

3.3.6 Cloud Computing

As energy production benefits from economies of scale when consumers transfer responsibility of energy production to an electrical grid for centralised production, so those needing ICT resources benefit from a move away from individual and fixed investment in local resources to exploiting cloud facilities. Clouds provide economy of scale and optimise resource use across multiple users and applications. Europe could gain significantly from new business opportunities afforded by clouds.

The EU, so it is claimed, lags behind the rest of the technology world when it comes to cloud computing. But there is enormous potential, which should not be lost. Early end-user engagement is vital in order to help direct investment and design. At the same time, of course, issues of trust and security cannot be overlooked, and need to be tackled together with interoperability and portability.

The barriers for the adoption of cloud computing within the FI ecosystem have been identified as:

- Lack of global legal framework: The global nature of cloud computing often with distributed assets indicates a need for some international cooperation and consistency

in laws across jurisdictions (e.g., data breach/notification). There is scope for involvement of international organizations on this matter, but it is important to ensure bottom-up feedback from users as well.

- Diverging definitions: Definitions of cloud computing vary greatly: some definitions refer strictly to infrastructure design while other definitions are broad enough to encompass nearly all online activity. The essence of cloud computing is the ability to provide a service on top of which users can create their own solutions.
- EU discourses focus on risk rather than benefits (see section 3.3.1 for more details): European conversations on cloud computing often focus on concerns and less on benefits (economic, business, etc.).
- Slow adoption of new technologies in EU context: EU is at times slow in adopting/focusing on new technologies; the prolonged focus on grid computing instead of cloud computing being an apt example.

The socio-economic challenges for cloud computing include:

- Increasing transparency and user-control: There is a need for more transparency and user control. Contracts vary greatly between different providers and often do not allow the user to control where his data is stored. In addition, many companies run services on a third company's cloud infrastructure. This may be unclear to the end-user who doesn't deal directly with the cloud provider yet relies upon the provider to secure the data and provide the actual computing service. Security in general is a concern; however, the perception of security by users is tightly linked to questions of transparency.
- Enabling portability while allowing customization: Designing interoperability/portability while allowing customization is a potential concern. Portability will allow users to move from one cloud provider to another; provide a more open marketplace and avoid platform lock in. The user can benefit from the infrastructure without knowing the underlying technology in detail.
- Disclosing meta-data use: Cloud providers can potentially gain a large amount of meta-data about the activities, locations, and contents of user interactions with their services. What data is collected and how it is handled could be better disclosed.

There are various strategies to bridge the gap and provide potential solutions:

- Enabling further development of sources of expertise around this 'young technology'.
- Building frameworks for knowledge exchange and closer connections between users, developers, and regulators.
- Facilitating increased interaction between Internet service providers and cloud providers. ISPs provide an essential underlying connection to the cloud, yet do not share in any revenue generation and are faced with an ever-expanding amount of data traffic.

3.4 Societal Priorities for the FI Ecosystem

The following tables identify eight cross-cutting societal priorities for the FI ecosystem which emerged from the discussions facilitated by SESERV between socio-economic experts and FI technology developers.

1.1 Call for increased transparency (data use and systems)	
Risk and Security	To reduce security risks through increased transparency requires that cloud service providers publish statistics, e.g., on monthly attacks. Transparency metrics are needed for users to determine 'trustworthiness' of providers.
Privacy	Increased access to transparent data on who has access to, e.g., online social network information can help users shape their behaviour. Transparency is often not desirable in the context of privacy questions. When propagating data, it might for example be better if peer-to-peer or information-centric networks are unaware of what information is transferred.
Identity	Systems should afford users increased transparency by offering advanced information filtering options.
Internet of Things	End-users should be clearly informed by providers about advantages and disadvantages of given Internet of Things technologies.
Online Communities	Transparent filtering options for users should be implemented for ease of self-management of interwoven and synchronised online networks. A transparent filtering option will assist users in managing smaller communities that align with cognitive limits of social ties (c.f. Dunbar's number[37]).
Cloud Computing	Cloud providers have access to meta-data of usage (locations, activities, content, interactions). How this data is used and stored could be disclosed better.

1.2 Call for more user-centricity and control	
Risk Security	Users have little scope for assessing and analysing security risks related to domestic ICT uses.
Privacy	Privacy principles are persuasive and propagate through the environment, influencing people's behaviour. More user-centric and user-influenced approaches are needed. User self-organisation and structure are important elements of social networks that must be acknowledged in design.
Identity	Users need better tools to help them manage/control how identities are shared and stored
Internet of Things	Users should be able to opt out of Internet of Things services. Different levels of 'sign-off' options should be available. User-centricity can be achieved if users are invited to have a role in design development.

Online Communities	Currently providers dictate terms of use; users lack influence and control. Creative uses by users should be fed into ongoing system/ application development.
Cloud Computing	Users should be able to control where their data is stored.

1.3 Continuing need for further multi-disciplinary and cross-sectorial bridging	
Risk and Security	Need for facilitating dialogue between technical and legal analysts to develop a better understanding of risks, and to assess new/future risks.
Privacy	Important to acknowledge different communities' expertise. Counter-movements such as ^mydex[38], DIASPORA*[39], and Internet of Subjects[40], should be seen as important sources of information. A gulf exists between practitioners and IT supply (e.g., practice driven innovation vs. principled approach).
Identity	Need for multi-disciplinary research on identity that can be translated into the design of socio-technical systems.
Internet of Things	Privacy research and IoT engineering are disconnected. Actors of the two domains should be brought together in the early stages of design. Policy makers should set up frameworks bridging the gap between IoT users and designers.
Online Communities	Examine frequency of multi-disciplinary conference, and possibly fund larger numbers of multi-disciplinary research centres.
Cloud Computing	Important to avoid silozation of cloud computing development and research. Initiating frameworks for knowledge-exchange between users, developers, regulators and researchers can help avoid silozation. ISP and cloud providers should develop stronger relationships. Revenues might be shared.

[38] http://mydex.org/our-service/what-personal-data-stores-do/
[39] https://joindiaspora.com/
[40] http://www.iosf.org/

1.4 Striking balances between outer-poles in debates and design	
Risk and Security	Not discussed
Privacy	eHealth privacy practices and discussions (e.g., patient records) could benefit from seeking a middle solution that allows proportionate access, rather than relying on either *laissez-faire* approaches or access over-formalisation (extreme regulation).
Identity	Important to allow for understandings and discussions of identity that acknowledge it as existing on a continuum ranging from stable to dynamic.
Internet of Things	Privacy concerns must be balanced against the potential value of Internet of Things technologies. There is a danger of moral panic in discussions on Internet of Things. Ethical considerations should stand central to discussions on Internet of Things potential.
Online Communities	There is a need to balance bottom-up and top-down technology development. New forms of communities or structures might emerge to drive design and development.
Cloud Computing	Not discussed

1.5 Facilitating further digital literacy development	
Risk and Security	Learning best practice and offering guidelines could help users assess and evaluate security and risk management related to their domestic ICT usage.
Privacy	Not discussed
Identity	Better digital literacy skills could equip users with more sophisticated tools for managing and understanding identity in online and hybrid contexts. There is a need to raise awareness of issues related to identity management.
Internet of Things	Involvement in early stages of design will help encourage and develop IoT experience and familiarity User concerns about IoT invasiveness would decrease with more experience
Online Communities	Providing further digital literacy education can help solve problems related to privacy concerns and management.
Cloud Computing	Not discussed

1.6 Addressing lack of common vocabularies and definitions	
Risk and Security	Not discussed
Privacy	Not discussed
Identity	Confusion about definitions. In the context of digital spheres, questions of identity are closely related to questions of privacy, data and rights. In broader societal contexts, identity is considered stable.
Internet of Things	Current definitions are too academic with too little focus on design and application. There is a need to develop vocabularies enabling discussions on multi-device Internet of Things interaction.
Online Communities	Indirectly addressed: need for vocabulary to address issues relating to health of networks/communities (e.g., development, growth, maintenance).
Cloud Computing	Current definitions are diverging: some refer exclusively to infrastructure, while others include social uses. It is suggested that Cloud Computing is understood in the context of providing a service on top of which users can create customized solutions.

1.7 Need for clarifying digital rights (including digital choice)	
Risk and Security	Not discussed
Privacy	Need for clarifying the right to full anonymity (e.g., in eHealth), while allowing for descriptors that can help identify emerging health issues.
Identity	Not discussed
Internet of Things	It is vital to provide offline access to IoT services to ensure that people are not penalized because of digital choices.
Online Communities	There is a need to address to what extent the right to have content/information permanently deleted should form part of a set of digital rights (what, e.g., about crimes against humanity?). Personal preferences should not be compromised when providers change their terms of use.
Cloud Computing	Not discussed

1.8 Inviting global regulatory frameworks	
Risk and Security	Need for streamlining legal frameworks across countries, or some providers might not offer their service there. In Italy, for instance, YouTube and Google are forced by law to take liability for their users. Providers who are not using measures that match local legislation might be discouraged. Need for determining approach to regulatory frameworks for distribution of security responsibilities for, e.g., cloud computing services: market-driven, self-regulating, or regulated?
Privacy	Not discussed
Identity	Not discussed
Internet of Things	Not discussed
Online Communities	Need for consistent regulatory framework which guarantees anonymity (conditionally / dependent on domain, e.g., politically sensitive topics).
Cloud Computing	There is a need for international cooperation and consistency in laws across jurisdictions (e.g., data breach and notification). It is important to ensure bottom-up feedback from users in this process

4 The FI Ecosystem and the Digital Agenda

For the European Union, ICT is seen as a beneficial factor in the future growth and development of Europe. The *Europe 2020*[41] initiative outlines the main challenges and opportunities facing Europe over the coming decade. In conjunction with this strategy, the *Digital Agenda*[42] has been developed to identify the immediate risks or challenges and to outline appropriate actions, including many aspects of the Future Internet. Since Internet-based activities, according to van Dijk[43], have a large impact on societal trends, the Future Internet deserves special emphasis. In this section we provide an overview of the digital agenda, the relationship with concerns from the FI Ecosystem and perspectives from project representatives in Challenge 1.

[41] The European Strategy for smart, sustainable and inclusive growth http://ec.europa.eu/europe2020/index_en.htm
[42] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:REV1:EN:HTML
[43] The European Commission (2010) *Study on the Social Impact of ICT (D7.1)* http://ec.europa.eu/information_society/eeurope/i2010/docs/eda/social_impact_of_ict.pdf ***and*** The European Commission (2010) *Study on the Social Impact of ICT (D7.2)* http://www.empirica.com/aktuelles/documents/International%20Comparison.pdf

4.1 What is the Digital Agenda?

The overall aim of the Digital Agenda is to “deliver sustainable and social benefits from a digital signal market based on fast and ultra fast internet and interoperable applications”. The Digital Agenda is in response to the Europe 2020 Strategy launched in early 2010 to prepare Europe for a “smarter” future, as it exits the economic crisis of the late noughties.

Figure 4: The "Virtuous Cycle” underpinning Europe's Digital Future [6]

At the centre of the Digital Agenda is the assumption that growth and innovation moving the ICT sector and thereby the European Union forward are part of a cycle of consumption driving technological improvement. This *virtuous cycle* runs something like this: if there are attractive services and content available online – and the content is assumed to be available uniformly across all member states – then this will motivate increased demand. More users will want to access the content and services, and will be looking for more and improved content and services. Increased demand in turn provides the necessary financial basis for improvements in the supporting infrastructure with increased bandwidth and speeds. This investment in turn enables ever more sophisticated service and content to be generated and supported, which, of course, then sets the whole cycle off once more.

Against a background of this profitable cycle, the Digital Agenda recognises that there are nevertheless a number of significant factors to be addressed. It identifies some seven major challenges or *obstacles*. These obstacles to European growth and development focus principally on infrastructure and the commercial structures surrounding its exploitation. Ultimately, the *virtuous cycle* can only continue to operate if the obstacles are addressed effectively. The Digital Agenda therefore responds to each obstacle with an individual focus area within which to group specific topics and actions. To a large extent, the obstacles represent *risks* to European advancement in the digital age. These risks are counterbalanced through the *opportunities* suggested by the Digital Agenda focus area.

The discussion in the previous section highlights that the relationship between the Future Internet and society is of interest to many different stakeholders with the increasing role of users identified as appropriate and useful from improving technology design to alleviating fears around privacy and security risks. There is no avoiding the fact that the social

aspects are therefore highly significant and should not be down-played within the context of the Digital Agenda. Nicola Dewandre[44], recently made two important observations:

- *all FI stakeholders should engage*: it is important to understand who the key stakeholders are in any piece of work or project and what their interests might be to avoid conflict; and
- *digital social sciences are vital* to be able to understand and sustain the appropriate user-centric growth and development of the Internet.

These are significant observations. Dewandre is highlighting the need to balance the concerns of users with the interests of network and infrastructures stakeholders. She is putting the emphasis back onto users and is specifically underlining the importance of looking to *how* users interact and adopt the technology – a subject for "digital social sciences".

4.2 How FI Ecosystem Priorities Address the "Obstacles"

The Digital Agenda defines seven obstacles to European advancement: fragmented digital markets, lack of interoperability, rising cybercrime and low trust, lack of investment in networks, insufficient R&D, lack of skills and fragmented answers to societal questions. The focus on infrastructure and cross-border eCommerce fails to acknowledge the importance of users and society. The base assumption of the *virtuous cycle* is that given the right environment and the right content and services, end-users will participate not least to consume. If that's the case, though, then there needs to be some considerable effort invested in at least understanding what and how people *use* services (or consume and generate content) along with any inhibitors to engagement with online activity.

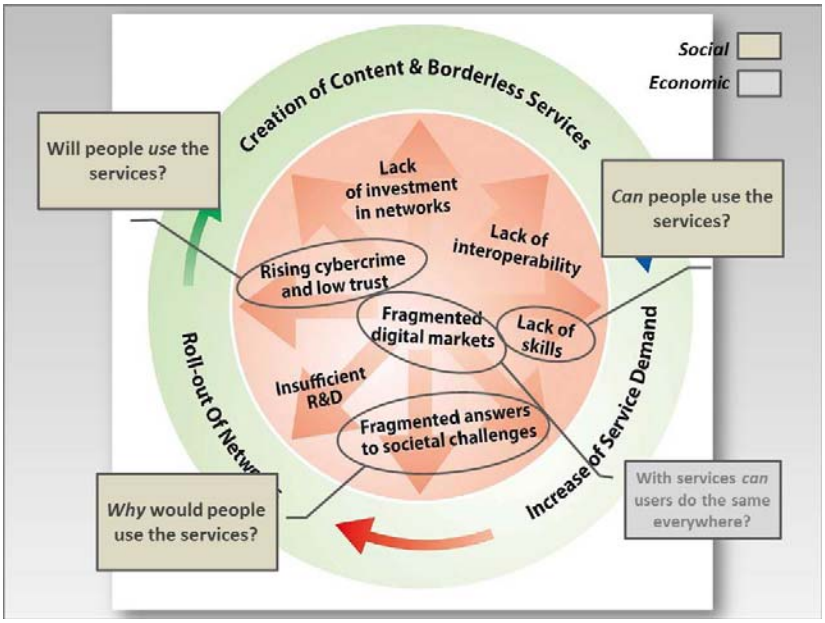


Figure 5: Obstacles of concern to societal aspects of the FI Ecosystem[45]

[44] N Dewandre (2011) The Societal Interface of the Digital Agenda for Europe Keynote address at the Oxford/SESERV Workshop http://www.seserv.org/panel/conferences-webcasts#dewandre

[45] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010DC0245R(01):EN:NOT

Figure 5 identifies key obstacles within the virtuous cycle and highlights the ones most related to barriers for users and society:

- Fragmented answers to societal questions - Why would people use services?
- Lack of skills - Can people use services?
- Rising cybercrime and low trust - Will people use the services?
- Fragmented digital markets – How can people using cross-border services be protected?

In the following sections we discuss these obstacles in relation to the FI ecosystem priorities identified in Section 3.4.

4.2.1 Obstacle 3 Trust and Security ~ Rising cybercrime and low trust

Will people use the services?	1.1. Call for increased transparency (data use and systems). 1.2. Call for more user-centricity and control. 1.3. Continuing need for further multi-disciplinary and cross-sectorial bridging. 1.4. Striking balances between outer-poles in debates and design. 1.5. Facilitating further digital literacy development. 1.6. Addressing lack of common vocabularies and definitions. 1.7. Need for clarifying digital rights (including digital choice). 1.8. Inviting global regulatory frameworks.

Participation in any shape or form, from consumption to engagement and social networking, will only succeed if issues around privacy and trust can be addressed. End users want assurance that what they do online is safe and secure. Protecting user credentials around a financial transaction is important but not the be all and end all. Content regulation especially in relation to minors is an obvious step, but also needs to include regulating access to certain content types, for example, keeping private and professional lives separate. An interesting observation from TAS3[46] concerns user notification of data access. Users were perfectly happy to share their content with others but they became more uncomfortable if they were shown who was accessing and viewing content, and how often. Similarly, the assumption that because large numbers of people are using social network sites, they will be happy to use it for other purposes such as commerce or eGovernment participation, may not be true[47].

Trust is an intrinsic property of all social interaction in real and online communities. It is no surprise that all FI ecosystem priorities contribute in some way to increasing the

[46] TAS3 project: see http://cordis.europa.eu/fetch?CALLER=FP7_PROJ_EN&ACTION=D&DOC=1&CAT=PROJ&QUERY=012d98b09089:f0ae:307fa6e1&RCN=85331

[47] Legislative Tensions in Participation and Privacy http://www.scribd.com/doc/55260687/Legislative-Tensions-In-Participation-And-Privacy

trustworthiness of the FI through principles of transparency, user control, multi-disciplinary dialogue, common vocabularies, and digital rights.

4.2.2 Obstacle 6 Enhancing digital literacy, skills and inclusion ~ Lack of skills

Can people use the services?	1.5 Facilitating further digital literacy development 1.6 Addressing lack of common vocabularies and definitions

Europe may rightly be concerned by a lack of skill to support all aspects of ICT, not least because so much in the public and private sector depends on it. 7% of the EU population has no computer skills whatsoever and more than 60% of people who are not educated beyond lower secondary level have no basic e-skills[48]. However, if users are unable or unwilling to make use of content or access services because of a lack of skill, then the desired virtuous cycle will grind to a halt, or at best become driven by a specialist, niche group of users. Usability and user acceptance will be key a critical success factor.

The Future Internet poses significant challenges for digital literacy due to the complex and dynamic nature of services and concepts. Look at any network diagram and you get a feel for the problem[49]. The problem is that decisions are being made in a world that is too complex for citizens to understand. People are overloaded with information, consequences are unknowable and also happen too quickly for them to react, even if they know what to do. Even concepts such as online identity go beyond a simple login. Users can choose what and how many personae they use for themselves when online, but they may also be forced into maintaining what appear to be multiple identities because of provider naming rules that prevent their normal identity from being allowed on another service. There is no strict limit to the number of identities or any specific cross-checking between them. A requirement to provide and support training around identity offers the possibility of helping end-users understand any exposures to them through online identity and thereby grow trust from the start. This may be a significant opportunity to explore: building trust through education. Projects which capitalise on practical experiences of users (such as those based around SNS's) or which make access in physical terms (exploiting pervasive consumer devices for instance) or make retrieval and access (search as well as aggregation) easier will do much in support of the digital inclusion objectives of the European Union.

4.2.3 Obstacle 7 ICT-enabled benefits for EU society ~ Fragmented answers to societal challenges

Why would people use the services?	1.4 Striking balances between outer-poles in debates and design 1.7 Need for clarifying digital rights (including digital choice) 1.8 Inviting global regulatory frameworks

[48] http://insight.eun.org/ww/en/pub/insight/policy/network/eskills_week_launch.htm
[49] http://www.ratemynetworkdiagram.com

The Digital Agenda highlights some of the challenges facing Europe and the rest of the world in the coming decades: climate change and an ageing population as well as the more prosaic goal to provide public services more efficiently online (e.g., the FI-PPP). However, this is a rather narrow view of how users have shown themselves to make use of the Internet. The success of SNS's can now be seen not only in terms of the numbers of subscribers, but also in that sites like YouTube, Ning and Foursquare are now being used for commercial purposes. There is more to how users exploit the Internet than suggested in the Digital Agenda. Projects need to understand how and for what purposes users engage online. Time and again, there is evidence that technology is adopted and then used in ways that were not originally anticipated: mobile phones are a prime example, where telephone calls may not be the main or primary purpose of the device.

The major problem for policy makers is that the Internet is a complex system and emergence is a key property. As with digital literacy, policy decisions are done in a world that is too complex for policy makers to understand. The consequence is that people have responsibility but cannot do their jobs properly. Established as well as *ad-hoc* communities are a significant force in present-day society, from the *Arab Spring* to tweets about super-injunctions. Failing to understand how they are used and what they mean to participants could have serious implications not confined to ICT policy. Online communities of all kinds are valuable sources of information about user concerns as well as usage. Strategists would benefit from some level of engagement with communities for direct or indirect feedback.

4.2.4 Obstacle 1 Digital Single Market ~ Fragmented digital markets

How can people using cross-border services be protected?	1.8. Inviting global regulatory frameworks.

Although difficulty in accessing and exploiting cross-border opportunities for content and services is largely seen as an economic issue, there are societal concerns. Data ownership, data protection and dispute resolution mechanisms across different jurisdictions that need to be considered in cross-border business transactions, especiallyB2C, all have societal impact. With the increasing use of services by consumers in other jurisdictions mechanisms that can help protect consumers when there is a dispute are important.

The set of available dispute resolution means is a key parameter in any type of contract. Dispute resolution provisions typically embrace questions of jurisdiction and applicable law. In cross-border business transactions (B2B or B2C), jurisdiction and applicable law are of special importance as jurisdiction refers to which state's courts have authority to hear and decide a dispute, while applicable law refers to which state's law is to be used in order to come to a decision.

Due to the principle of state sovereignty, each state may define its own Private International Law (PIL) governing the state-specific set of connecting factors based on which their own or foreign jurisdiction is established, application of their own or foreign law is substantiated, and recognition of foreign decisions is granted or denied. This territorial

approach to dispute resolution makes PIL a highly complex field of law, in particular in an increasingly international and digital economy.

This is why several efforts in harmonizing PIL have appeared. For member states of the European Union (EU), for instance, the two main harmonized PIL instruments are the Brussels I regulation[50] (for questions of jurisdiction) and the Rome I regulation[51] (for questions of applicable law). Despite ongoing harmonization endeavours in different regions and in different bodies, previous research reveals that fundamental challenges in handling dispute resolution remain essentially unaddressed in market places which are *a priori* border-less— the Internet being a prominent example.

To investigate dispute resolution, a number of steps were investigated. On the one hand, a system to produce a list of recommended jurisdictions for the contract of an electronic service in the Internet — e.g., a content service — in an automated manner was designed and implemented as a prototype. To this end, a method to formally model PILs in a machine-executable way, and to implement the respective jurisdiction-oriented reasoning was determined. In order to show the feasibility of this approach, as well as its limitations, the Brussels I regulation was modelled and implemented[52]. The approach has proven fully functional *per se* but even with regionally harmonized PILs like the Brussels I regulation in place, scalability on a global scale remains challenging due to the considerable modelling and implementation effort for each PIL to be covered. In addition, questions of conflicting recommendations and mutual recognition among modelled PILs have not been addressed. In essence, this approach shows that the territoriality principle, while it would clearly suffer from severe issues of PIL, may be supported to some extent in the Internet with PILs of as many states to be modelled and implemented as exist to date.

On the other hand, a comprehensive comparative analysis of the PIL situation in the USA, the EU, and in China resulted in the identification of service provider market activities that may constitute jurisdiction in those regions investigated[53]. To that end, the set of region-specific connecting factors was compiled and assessed based on a common frame developed for comparison. Connecting factors were mapped to service provider market activities in the Internet (e.g., targeted on-line advertisements) and the real world (e.g., presence by means of distrainable property). The assessment of techno-legal implications that was conducted as a result revealed that both service providers and service customers are confronted with a high level of jurisdictional risk and uncertainty in dispute resolution when doing international electronic business in the Internet. In essence, this research effort shows that the current approach to cross-border dispute resolution as reflected by the PIL of today fails for international electronic business in the Internet.

---

[50] Council of the European Union. Council Regulation (EC) No 44/2001 of 22 December 2000 on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters. Official Journal of the European Communities, L12:1–23, Jan. 2001.

[51] European Parliament and the Council of the European Union. Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the Law Applicable to Contractual Obligations (Rome I). Official Journal of the European Union, L177:6–16, July 2008.

[52] M Waldburger, M Charalambides, T Schaaf and B Stiller. Automated Determination of Jurisdiction and Applicable Law for International Service Contracts: Modeling Method, Information Model, and Implementation. In 18th Biennial and Silver Anniversary International Telecommunications Society Conference (ITS 2010), pages 1–31, Tokyo, Japan, June 2010.

[53] M Waldburger, A Macri, and B Stiller. Service Provider Market Activities Constituting Jurisdiction for International Service Contracts— A Structuring Approach and Techno-legal Implications. In 21st European Regional ITS Conference (ITS 2010), pages 1–22, Copenhagen, Denmark, Sept. 2010

Therefore, a transition towards a single, internationally harmonized PIL for electronic business in the Internet is perceived as the dominant long-term strategy in order to foster certainty and trust in international electronic business substantially. Such transition needs appropriate identification of the interests of stakeholders which may take time as it involves a large number have differing agendas, interests, and objectives.

4.3 Technologists' Perspectives on the Digital Agenda

Raising the awareness of the Digital Agenda within the Future Internet community is essential. It is clear from community discussions that knowledge of the aims and relevance of the focus actions is variable across many of the projects and participants. A number of community participants were interviewed informally to get some feel for how projects themselves view their contribution to the overall European focus on innovation and the role of ICT in society[54]. The objectives of the consultation were:

- to identify gaps between the regulatory frameworks defined on a regional level by the European Commission and the practical implementation of these guidelines by different research communities that work in the Future of the Internet;
- to give voice to the stakeholders: It was considered relevant to provide visibility of different socio-economic research that is studying or implementing innovative practices to develop the Future of the Internet. This was considered relevant for the internal FIA community but also for other sectors of society;
- to facilitate the comparability of perspectives: In order to provide a 'panoptic view' of different perspectives and experiences all the interviewees answered the same questions (see below). There are, of course, no right or wrong answers but the diversity of viewpoints was considered important to be disseminated; and
- to identify the relevance of the Digital Agenda: Given the background of these participants and the proximity of their work to several themes included in the EU Digital Agenda it was considered important to see how familiar they might be with this EU instrument and also to understand the value that it provides to their current activities.

Although the number of interviews was limited and cannot be construed as representative of the whole community of technology providers, some common observations can be made and themes extracted.

How do you think projects benefits a broader European drive to increase innovation?

For some of the projects, their work addresses needs which have not really been understood before such as connection reliability in remote areas with little infrastructure, or in response to societal challenges as a result of on-going social trends, such as the fragmentation of family units through economic or other migration. Further, that some technology needs research and to be developed not for commercialisation, but rather to seed follow-on innovation.

[54] The interviews are available online at: http://www.seserv.org/panel/videos-interviews

What are the main social and economic problems, constraints or barriers?

Problems of connection and access as well as social fragmentation (see above) are perceived as relevant issues to be studied and addressed. But more than this, many of the projects recognised that they were enabling social interaction and other benefits by creating appropriate frameworks and infrastructures. Leading on from this, and providing indirect support to the Social Impact studies, the view was expressed that there is in actual fact no distinction between technology and the society that uses it. Interestingly, there was a lone voice that suggested that provided the technologists are suitably skilled and experienced, there is little contribution to be made by social scientists. Ultimately, though, it seems that there needs now to be less research and development effort within the area of technology *per se* and more focus on the application and use of technology in a social context.

Who are the stakeholders? Why are they important?

There is often little thought behind who the stakeholders in projects really are. Often, it is either just the partners (the project consortium) and/or the investors and regulators who are seen as the primary stakeholders. However, limiting the stakeholders in this way is very risky: unless the end-users or communities are included, then they have no representation and all too often the societal relevance of the technology generated is lost or simply misunderstood. The latter approach – where stakeholders include the ultimate beneficiaries of the project – does lead to relevant and appropriate debate around other, related issues that can only be of benefit to the project itself but more importantly to the wider community[47].

What is known of the EU Digital Agenda? How is the Digital Agenda relevant?

It was noticeable that there was little widespread understanding of the content or intention of the Digital Agenda among the projects. Europe may set its agenda and indeed provide the appropriate motivation for technology research and advances, but there is either little understanding among the projects of what it means and why it is relevant or, perhaps more importantly, there is a perception that government and the EU should not seek to micro-manage projects, their goals or how they proceed: if innovation is to deliver, then a significant amount of freedom and autonomy is required. Notwithstanding such views, there was a general consensus that the Digital Agenda is important in taking Europe forward in technology as well as socially, though there was some concern that it may be too high level and lacking global relevance beyond the EU. The projects did feel, however, and this was echoed in the discussion following Nicole Dewandre's keynote speech[44] , that technologists and social scientists do have much to contribute to the Digital Agenda as an instrument for outlining future strategy.

What mechanism or strategies are needed to foster research (either from the public sector or from other entities)?

The Digital Agenda does highlight the problem of a lack of skill, both for end-users as well as ICT professionals. A number of projects echoed this concern. Although there is significant skill in some technical areas, the areas of design and application seem to be particularly problematic. Taking this a step further, participants were keen to see the encouragement and support of cross-disciplinary approaches. It would be particularly beneficial to invest in the development of appropriate tools to support both design and more general usage and implementation investigation.

The common themes identified where:

- *Understanding stakeholders:* many of the projects interviewed focused solely on direct controlling parties, those providing the funding, regulators and the consortium partners themselves. This means that some relevant considerations are missed, not least in considering the specific impact of the technology on those who will use or be affected by it. This needs to be considered on a project by project basis. In respect of the overall view presented earlier (Section 3.2), it is important that the projects identify which stakeholders they impact with the technology they are producing, directly and indirectly. This point was stressed in Dewandre's keynote address[44]: all stakeholders should engage. If nothing else, the problems of those stakeholders may lead to creative and innovative pragmatic solutions. The question for the projects, then, is who are the stakeholders and how are they affected by the technology produced?
- *Understanding the relevance and importance of the Digital Agenda* as well as the *Social Impact* studies[43]. The *Digital Agenda*, if familiar at all, tends to be seen as remote and irrelevant to specific topics within the projects themselves. Given the associations between the *Digital Agenda* setting out the areas of ICT R&D and the *Social Impact* studies examining the effects of that technology, then relating the work back to the *Digital Agenda* can help to uncover the societal risks and opportunities (the constraints as well as benefits) that the technology produced may have. For the projects, then, we need to relate the projects' aims and deliverables back to the *Digital Agenda* and the *Social Impact* studies.
- *Skill (both ICT and end-user):* the *Digital Agenda* highlights a significant risk here and proposes to "enhance […] digital literacy, skill and inclusion". The point is, according to the *Digital Agenda*, that on the one hand we need increasingly more technical and sophisticated ICT skills to be able to support the systems we have, as well as to counter any malicious attack, not least because of the sensitivity and critical nature of the services and systems supported by ICT; and on the other hand, a lack of digital training is regarded as an inhibitor to the generic goal of comprehensive inclusion. However, there may be a third and more significant aspect to skill level. Studies by Dutton and his colleagues concerning cybertrust suggest apart from anything else that increasing familiarity through higher Internet use increases levels of trust as users become more comfortable with what they can and should not do[55]. Skill may, therefore, go beyond simple connection; with suitable training and experience, users will certainly be able to appreciate the implications of their online activities and may even become better equipped to assume responsibility for controlling their own online presence. The issue for the projects, therefore, is whether training can help empower users to take greater responsibility for themselves.
- *Cross-disciplinary collaboration:* As Internet actors change (cf. Figure 3), moving away from infrastructure-centric (the "traditional actors") to a user and services focused view (the "emerging actors"), then it is no longer clear that the ecosystem of the Internet is now principally based on engineering excellence. For the *virtuous cycle* of the *Digital Agenda,* it is not sufficient to attract investment in the networks; a key element is the development of content and services which need to attract consumers. If those consumers are not "digitally literate" to the extent of ICT professionals, then attraction will be based on other factors and not just engineering elegance. Once end users

[55] Dutton, W.H. and Shepherd, A. (2003) "Trust in the Internet: The Social Dynamics of Experience Technology", The Oxford Internet Institute, available from: http://www.oii.ox.ac.uk/resources/publications/RR3.pdf

become involved though, attracted by suitable and user-centric design, then *they* will dictate how they wish to engage and how they expect to interact with a given service or content. Understanding their expectations and how they use the technology is more an issue of the *Social Impact* studies rather than infrastructure, beyond simple questions of connection speed, bandwidth and access. Subscribers to SNS's have expectations on how they wish to interact with friends and family online, which may not sit well with the commercialisation of the environment or with economically driven approaches to privacy. The question for the projects then would be whether and how they might benefit from insights from other disciplines.

4.4 The Challenge for Policy Makers

In general the societal concerns identified can be simplified to a model of consumers, providers and regulators. *Online Communities* may be identified as consumers; *Cloud Computing* and the *Internet of Things* as infrastructures can be seen as "Providers"; and the remaining concerns – *Online Identity, Security* and *Privacy* – relate to the rights (human rights and digital rights) and regulatory controls which seek to protect and guide deployment.

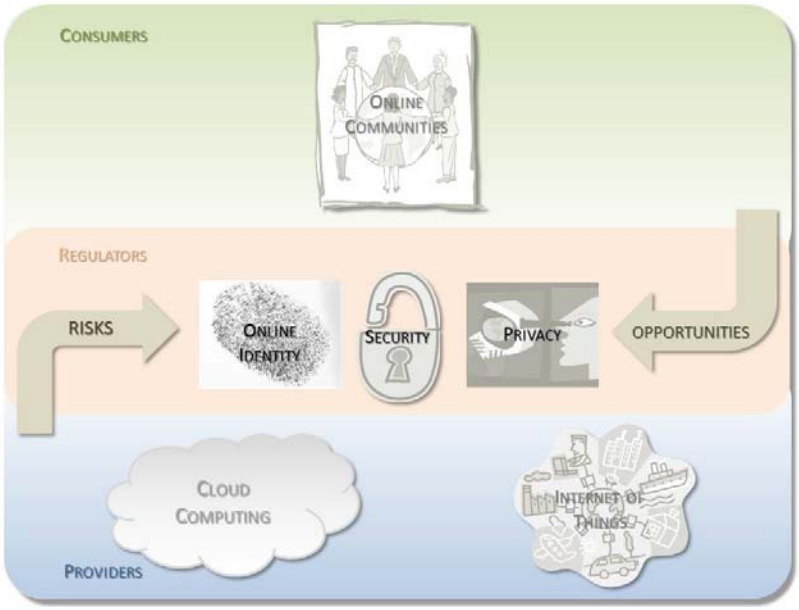


Figure 6: The Challenge for the Regulators

Policy makers have a number of choices in relation to the societal concerns identified within the FI ecosystem. They can, for instance, be prescriptive and impose legislation on consumers and providers. The intention, as presumably with all legislation, would be to provide clear and unambiguous guidelines of what providers can and cannot do when they offer services or infrastructures either to ensure safety or address market failures. It is then up to them to comply. There are practical problems to be overcome here, of course, not least in connection with cross-border jurisdiction and a lack of experience amongst users. But more significantly, the imposition of legislation may stifle significant advances in other areas.

An alternative to legislation would be to look to the consumers themselves. Users can be assumed to have their own expectations with respect to privacy and data protection. Initially, users seem to have believed that they were in complete control of who could view

what when they posted information on line. This was not the case: the much-publicised *facebook* changes for privacy settings have come from user dissatisfaction rather than an attempt at regulatory control.

Consequently, regulators seeking to control and protect need to constantly consider real usage. In adapting to the concerns and activities of the real consumers of a service, as consumers, prosumers or contributors, there is some benefit to be gained from examining the practical *status quo*. Involving the online communities is important not least because they are real stakeholders within the Future Internet ecosystem. In addition, they provide valuable insights into how technology can be and is being used in practice, as well as what the users expect. At the same time, reviewing real usage provides some understanding of those areas where end-users could profit from support and education, not least to allow them to assume appropriate levels of responsibility for their own actions.

5 Conclusions

This report has presented the opinions and views of social scientists and technologists working on the Future Internet in respect to societal priorities. The concerns and challenges discussed and possible future strategies and priorities where selected by the community themselves. The results represent a snapshot of the challenges facing technologists undertaking Future Internet research.

There is no doubt that the FI ecosystem is an increasingly rich, diverse and complex environment to study. The FI stakeholder analysis shows how the Future Internet will touch almost all aspects of society way beyond what was envisaged by the Internet Society in 2009. Challenge 1 projects are aware of key societal concerns within aspects of FI ecosystem, how potential technological solutions can address them and also what challenges lie ahead. As a consequence, eight societal priorities have been identified:

- 1.1. Call for increased transparency (data use and systems)
- 1.2. Call for more user-centricity and control
- 1.3. Continuing need for further multi-disciplinary and cross-sectorial bridging
- 1.4. Striking balances between outer-poles in debates and design
- 1.5. Facilitating further digital literacy development
- 1.6. Addressing lack of common vocabularies and definitions
- 1.7. Need for clarifying digital rights (including digital choice)
- 1.8. Inviting global regulatory frameworks

In contrast, the Digital Agenda is not deeply understood by technologists. There is a gap between a set of high level policies and incentives that are particularly focused on infrastructure and complex regulatory processes and the society that is using or will use the technologies being developed. It seems that these regulations ignore some of the citizenship concerns and there is a clear disconnection in this instrument. From discussions with Challenge 1 projects it was quite clear that not even the ‘stakeholders’ of the Future Internet are fully aware or interested in the Digital Agenda.

The EU Commission needs to find a way to design and update a Digital Agenda that responds to the necessities of a broad spectrum of people and communities (not only the

big organizations, companies or government). For instance, the rural and remote regions, the non-organized communities and even SMEs seem to be underrepresented in this 2020 policy action. In other words, design different 'soft' mechanisms that help the Digital Agenda to adapt to the social, political, educational, labour, and environmental needs of the community, not only for 2011, but iteratively for this decade. If the Digital Agenda is not embedded in the principles of openness, adaptability, participation and transparency it is hard to believe that it will succeed (e.g., Lisbon Agenda).

Overall the 1st year social coordination activities have offered an opportunity for Future Internet community participants to share views on how technology can address societal concerns. It is clear that the complexity of the issues discussed requires face-to-face interaction to ensure effective communication of conceptualisations and ideas. Structured workshops with participation from key community stakeholders offer far better results than relying on an analysis of EC project documentation or survey results. The second year will continue engagement through dedicated workshops and focus groups building on the results of the first year and future thoughts discussed in the following section.

6 Future Thoughts

SESERV was motivated in 2009 by the following arguments:

> *"After 10 years of economic growth the world economy is in a crisis. Fundamental questions are being asked about the society, the economy, and how ICT (Information and Communication Technology) can help to support a sustainable Europe in the context of an increasingly connected world. Technical innovation in the Internet today has been motivated by the belief that macro-economic growth will drive wealth creation, growth will continue and this will attract investment whilst helping all aspects of our society. In response, ICT research has developed technologies to reduce costs and increase economic activity by creating faster networks, improving automation and system intelligence. Although efficient economic activity is important it is still not clear that the advances in technology are sufficient to reduce environmental impact and help society escape its problems[56]. According to ecological economics, continued macro-economic growth is not sustainable due to ecological constraints and, as in micro-economics, there is a "tipping point" where the cost of increased economic activity is not worth the expense[57]. Today, aggregate growth is now in many cases costing us and lowering, rather than improving, welfare. In fact, at some point, the world economy will need to operate with growth levels close to zero, but that makes it very difficult to sustain western-style free-markets, where investment is motivated by confidence/trust in future growth. This leads to basic questions about how to incentivize economic activity in the emerging digital economy?"*[58]

Since 2009, societal, economic and environmental events show that society continues to grapple with these tricky issues. Today's population uses 50% more resources than the planet can generate and consumption has doubled since 1975. "There is no credible sustainable solution which is also a desirable option" said Jack Jacometti (Shell Int) at the

[56] M. Chertow: IPAT equation; In: Encyclopedia of Earth. Eds. Cutler J. Cleveland, Environmental Information Coalition, National Council for Science and the Environment, Washington, D.C., 2008. http://www.eoearth.org/article/IPAT_equation

[57] H. Daly, E. Elgar: Ecological Economics and the Ecology of Economics: Essays in Criticism; Edward Elgar Pub, Cheltenham, U.K., 1999.

[58] SESERV Description of Work

recent Paradiso conference on Internet and Societies[59]. More dramatically, according to Marc Luyckx Ghisi (former member of the "Foresight Studies Unit" of the European Commission's Presidency), “We are witnessing a change in civilisation, the public do not believe in current socio-economic structures and with lower trust the industrial/capitalist systems are over”[60]. Economic progress is not delivering an increased quality of life and new value structures that consider qualitative measures may be needed to provide incentives for societal behaviour change.

The EC PASHMINA project[61] has questioned the dominance of the economic route through four scenarios across the dimensions of speed and levels of collaboration: Growth without limits, growth within limits, turbulent decline and stagnation and new welfare. Growth without limits is the current vision and cannot continue they argue. PASHMINA proposes a new welfare model building on qualitative human development, human rights and also natural right (well-being and sustainability indicators). Such a model would aim to increase peer-to-peer relations as opposed to hierarchical structures, increasing awareness and cognitive autonomy, support collective intelligence and responsibility of sustainability, promote freedom of action and empowerment, and enable security with others. These objectives are directly aligned with priorities for the FI ecosystem but go far beyond them. Research will increasingly need to focus promoting the value of network and social capital rather than the continuous drive for economic efficiency and consumption (e.g., virtualisation).

None of the visions address the clear tension between the altruistic characteristic required for common good and selfish natures of private interest. It seems unrealistic to believe that society will suddenly move from individualism to a digital utopia of shared community values enabled by a Future Internet. Many businesses, individuals and states will no doubt remain self-interested. What is apparent is that we are transitioning from a world of abundant resources to a world of constraints. The consequence will be the need for increased personal responsibility and empowerment in aspects of lifestyle such as energy, public services and health. The Future Internet and in more general ICT have great potential to help. “Today we see location-based monitoring […] used to protect fisheries, financial systems distribute farm subsidies, satellite images help control diamond mining and mobile technology supporting participative sensing for carbon footprints monitoring” says Stefan Lechner, Director Institute for the Protection and Security of the Citizen, JRC Ispra[62]. But many recent innovations have focused on maximising utilisation and increasing consumption. Technology and business models designed to offer unlimited[63] access to commodity resources such as elastic clouds will become more constrained in future.

The Future Internet can help society manage complex and collective problems. However, without a change in societal belief structures any single solution is subject to the displacement effect. Consumers may spend their energy savings on new products and services, home workers may heat their entire homes less efficiently than shared offices. Systems must be designed to consider the total impact and this is where methodologies

[59] http://paradiso-fp7.eu/events/2011-conference
[60] http://paradiso-fp7.eu/wp-content/plugins/alcyonis-event-agenda//files/ICT,-a-New-Civilization.pdf
[61] http://www.pashmina-project.eu
[62] http://paradiso-fp7.eu/wp-content/plugins/alcyonis-event-agenda//files/ICT-against-Resource-Misuse.pdf
[63] All resources are limited but to the consumer of cloud services capacity limits are not their concern so long as then have funds to pay.

such as Tussle analysis, which considers possible spill overs, may have value. Of course predicting outcomes, desirable or otherwise, is increasingly difficult within such complex systems. This was highlighted as a major challenge in the earlier discussion on Risk Management (Section 3.3.1) and Obstacle 7 (4.2.3). Policy decisions are made in a world that is too complex for policy makers to understand and too dynamic for timely responses. In many circumstances consequences of actions will not be fully understood and there's a tendency to be reactive. Taking action in such an uncertain environment will require greater reliance on experimentation in contrast to design, new ways of measuring success that consider greater chances of failure and helping all FI ecosystem stakeholders to determine their appetite for risk.

Many experts are calling for research and development that takes a holistic approach and systemic thinking. This has prompted the creation of the European Internet Science Network of Excellence (EINS)[64]. The objective is to work towards establishing a scientific basis for Internet research that can help in studying the Internet, developing methodologies for FI systems research and enabling effective discourse between different disciplines. EINS takes a multidisciplinary approach that builds on the principles of network science combined with other disciplines from a wider social and legal context such as economics, sociology, psychology and complexity.

Understanding the nature of, and influencing and managing Internet networks is key for societies. Metcalf's law states that the network value scales two times the number of persons connected[65]. Recent examples from China in response to a crisis event show the value of micro blogs used by both citizens and governments[66], although censorship of some posts caused anger. Networks do have huge value and making them larger is the goal for all service and infrastructure providers. However, as with all technology, networks can be perceived to have both positive and negative societal consequences. Critiano Codagnone, Senior Scientist, JRC / IPTS, noted that "Networks can change the norms of acceptability, for example, greater obesity and alcohol consumption in some western societies is actually a network problem"[67]. This leads to the ongoing debate about embedding specific values in the Internet architecture[68].

In this context, the goals of SESERV remain highly relevant. Maintaining focus on assisting technologists in their understanding of the potential impact of FI technology along with barriers and strategies for adoption through dialogue with social scientists is increasingly important. The challenges facing society are larger than ever and the Future Internet will surely be an integral part of possible solutions. However, to realise the benefits all stakeholders will need to continue in discourse between those that study and those that build the Future Internet. Having identified key issues and challenges in taking Europe forward towards an appropriately informed and shaped Europe 2020, SESERV will continue and grow engagement seeded in the 1st year. Capitalising on the benefits and success of the SESERV Oxford Workshop, in the 2nd year, SESERV will take the debate to the technologists and social scientists in their own environment: we have identified the issues, and can now facilitate more focused discussion through focus groups meeting at

[64] http://cordis.europa.eu/fp7/ict/fire/internet-science_en.html
[65] http://en.wikipedia.org/wiki/Metcalfe%27s_law
[66] http://www.theepochtimes.com/n2/opinion/microblogs-shed-new-light-on-chinas-train-crash-59803.html
[67] http://paradiso-fp7.eu/wp-content/plugins/alcyonis-event-agenda//files/ICT-Building-Resilience-Within-Societies-Smart-Health.pdf
[68] I. Brown, D.D. Clark, D. Trossen, "Should Specific Values Be Embedded In The Internet Architecture?", http://conferences.sigcomm.org/co-next/2010/Workshops/REARCH/ReArch_papers/10-Brown.pdf

other FIA events exploring concerns raised already, but against a background of the need to consider carefully new social paradigms for future prosperity outlined by PASHMINA and Paradiso.

7 Abbreviations

B2B	*Business to Business*
B2C	*Business to Consumer*
BRIC	*Brazil, Russia, India and China*
CNO	*Collaborative Network Organisation*
DDoS	*(Distributed) Denial of Service*
DTN	*Delay- and Disruption Tolerant Networking*
EC	*European Commission*
EU	*European Union*
FI	*Future Internet*
FIA	*Future Internet Assembly*
FI-PPP	*Future Internet Public Private Partnership*
FP	*Framework Programme*
GP	*General Practitioner*
ICT	*Information and Communication Technology*
IoT	*Internet of Things*
ISP	*Internet Service Provider*
PDA	*Personal Digital Assistant*
PIL	*Private International Law*
PPP	*Public-Private Partnership*
R&D	*Research and Development*
SME	*Small to Medium Enterprise*
SNS	*Social Network Site*

8 Acknowledgements

This deliverable was made possible due to the large and open help of the SESERV consortium, members of the FISE-WG and other Challenge 1 projects. The authors would like to thank:

- SESERV partners George Stamoulis (AUEB), Costas Kalogiros (AUEB), Didier Bourse (Alcatel Lucent), Daniel Field (ATOS)
- All FISE-WG members who have contributed over the past 12 months

The authors gratefully acknowledge the support of the following during the SESERV workshop in Oxford:

- *The keynote speakers*
  - Professor W. H. Dutton, Oxford Internet Institute
  - Nicole Dewandre, European Commission
- The debaters
  - Dr Jonathan Cave, RAND Europe, FI3P
  - Professor Robin Williams, University of Edinburgh
  - Professor, Maastricht University

- *The facilitators*:
  - Professor Christopher Millard, Oxford Internet Institute
  - Dr Ian Brown, Oxford Internet Institute
  - Dr Sandra Gonzalez-Bailon, Oxford Internet Institute
  - Ben Bashford, Bashford LTD, COUNCIL
  - Tony Fish, AMF Ventures
  - Dr Mike Surridge, University of Southampton IT Innovation Centre
- *The scribes*:
  - Scott Hale, Oxford Internet Institute
  - Chrysanthi Papoutsi, Oxford Internet Institute
  - Bianca Reisdorf, Oxford Internet Institute
  - Lucy Power, Oxford Internet Institute
  - Isis Hjorth, Oxford Internet Institute
  - Nesrine Abdel-Sattar, Oxford Internet Institute
- *Those interviewed:*
  - Ben Bashford, Bashford LTD, COUNCIL
  - Elwyn Brian Davies, Folly Consultancy Ltd, N4C
  - Kevin Doolin, TSSG, SOCIETIES
  - Magnus Eriksson, Interactive Institute, TA2
  - Ian Graham, University of Edinburgh, MyFIRE
  - Peter Ljungstrand, Interactive Institute, TA2
  - Daniel Sebastião, Instituto de Telecomunicações, SAIL
  - Martin Serrano, TSSG, SOCIETIES
  - Mike Surridge, IT Innovation, GENESI-DEC
  - Nick Wainwright, HP, EffectsPlus

9 Appendix I: Societal Project Reviews

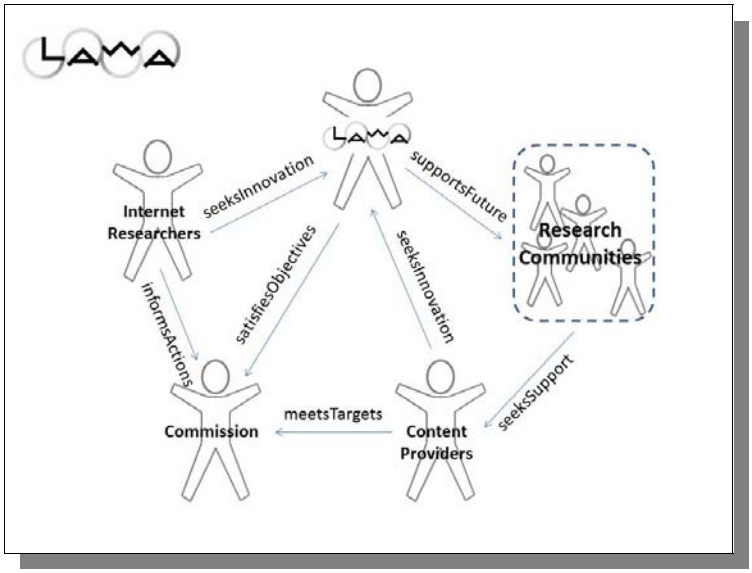
In all, seven projects were selected for their societal concerns covering FP7 project challenges 1, 7 and 8.

Project	
9.1.1 LAWA *Test facility* Objective 1.6	The LAWA (Longitudinal Analytics of Web Archive) project is specifically concerned with understanding all characteristics relating to FI content (its size, form, structure, distribution, dynamics and provenance). The project offers test facilities for those working in these areas.

Website: http://www.lawa-project.eu

FI Importance: The project is essential to foster a greater understanding of long term data storage. In addition, it offers an opportunity to test some of the trust and identity issues associated with long term data retention.

Stakeholders:



External relevance:

Digital Agenda	***Societal Trend(s)***
DA Columns: 5, 6 and 7 *Opportunity*: supports analysis and management of content,	Feeds directly into the *Information and lifelong learning* theme across domains, and has some relevance for the *Culture*

	and so important for the preservation of heritage at least. *Risk*: content crawling could be regarded as intrusive.	and *Daily Life* trends. The main societal benefits associated with a LAWA-type test facility is enhancing search capabilities to find and interact with information and content.

Community relevance: *From the Oxford Workshop* It was clear from the breakout discussions on *IoT* and *Online Communities* that end-users need training to understand the implications of posting content online, but at the same time would wish to see more control, not least for themselves, of how and where information as used as well as when it is made available beyond the immediate context within which it was first made available. The discussion around digital erasure (the "right to be forgotten") is perhaps especially pertinent.

9.1.2 SENSEI

Development framework

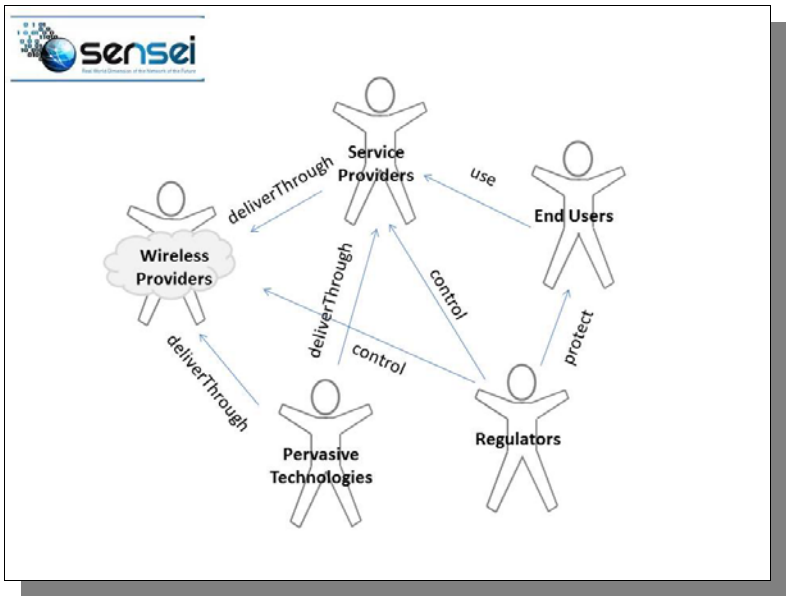
Objective 1.1

Provides an open, business-driven architecture for the development of services and applications using heterogeneous wireless sensor and actuator networks, including a high level of context-awareness for real-world interactions. Also includes appropriate security and privacy measures for users.

Website: http://www.ict-sensei.org

FI Importance: IoT is one direction that the FI may develop, not least because of the prevalence of powerful personal data and communication devices. Addressing associated functional and non-functional aspects now is essential for the FI.

Stakeholders:



External relevance:	***Digital Agenda***	***Societal Trend(s)***
	DA Columns: 1,2,3,4 and 7 *Opportunity*: creation of a pervasive and non-intrusive infrastructure for the development of new services and content. *Risk*: may not extend to all areas or populations: digital inclusion may not be served.	This affects *all* themes in the *Social Impact* studies, especially *Rationalization* and *Networking and social capital*. SENSEI adds to the ways in which users can access and interact with online service and content.

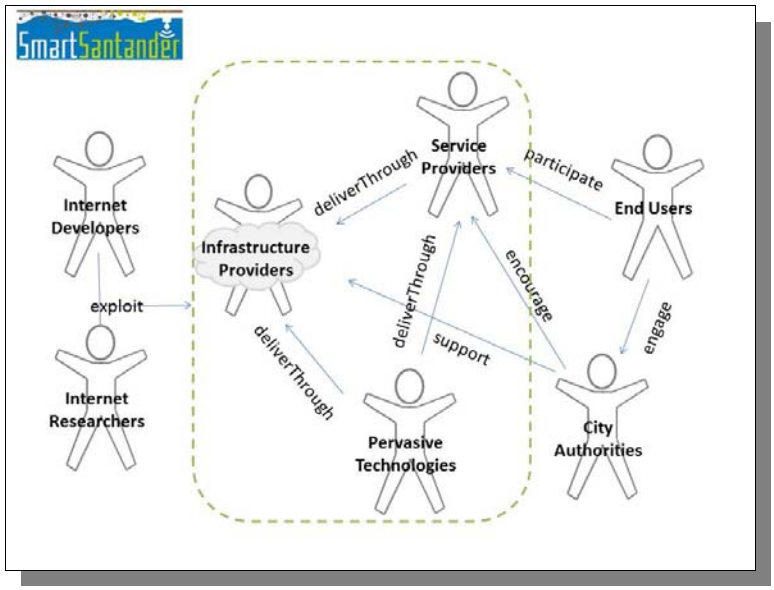
Community relevance: *From the Oxford Workshop* and specifically in relation to the discussions on *IoT,* there is a clear desire for end-user participation in the design and development of technologies within this arena to help alleviate the inherent caution and mistrust associated with pervasive devices.

9.1.3 SmartSantander *Test facility* Objective 1.6	Provides a test facility for *smartcity* applications and services, to encourage the development of appropriate participative sharing and IoT-type applications.

Website: http://www.smartsantander.eu

FI Importance: Testing IoT-type services and applications in a real but controlled environment will help identify what needs to be taken into account for FI smart environments.

Stakeholders:



External relevance:

Digital Agenda	***Societal Trend(s)***
DA Columns: 4,5 and 7 *Opportunity*: support for participative activities within a real urban environment for all aspects of digital inclusion. *Risk*: may lead to issues of trust and concerns over privacy; related issues of traceability and trackability.	Services and applications developed in a *SmartSantander* type setting support all themes of the *Social Impact* studies, and all of the domains they propose. These services are all about inclusion and enablement for *whatever* societal purpose the user comes up with. Potentially, the benefits are enormous.

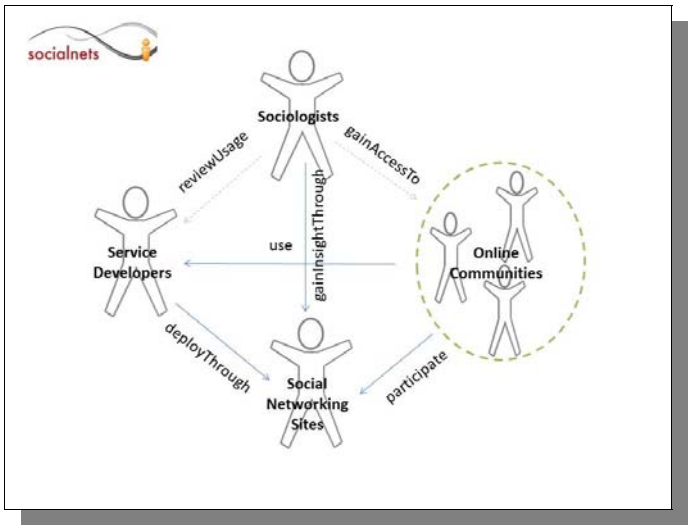
Community relevance: *From the Oxford Workshop*, it is clear that there is some nervousness around *IoT*-based services among end-users. Facilities like *SmartSantander* provide an opportunity to involve users at all stages in the development and testing of technology which may support the need for education and training, but also to show the potential of these technologies in benefiting the community and society at large.

9.1.4 SOCIALNETS *Opportunistic community building* Objective 8.2	Exploiting SNS to deliver as well as acquire content, with appropriate support to ensure security and trust. The project looks both at online SNS, as well as opportunistic wireless networks. In addition to the primary aims around SNS and content provision, the project has provided useful research material in understanding cyber interaction between individuals within groups.

Website: http://www.social-nets.eu

FI Importance: Online communities represent an engaged and relatively skilled audience who can inform future design and policy decision around the FI.

Stakeholders:



External relevance:

Digital Agenda	***Societal Trend(s)***
DA Columns: 3 and 7 *Opportunity:* Studying information about usage and behavioural patterns within an SNS-type context offers essential information to all in ICT on how to engage with consumers and ensure the technology developed is appropriate. *Risk:* Opportunistic networking may represent confirmation of the	SNS have a significant influence on contemporary life: it is not just about interpersonal relationships, instead it has become a "democratizing influence" to support all kinds of engagement. *Studying* SNS usage and behaviours can only benefit understanding of how technology can be and is used; exploiting it for commercial gain may satisfy some of the *Social*

	reluctance to engage with IoT type services. SNS participants may feel uncomfortable that investigation or commercial service delivery is intrusive.	*Impact* domains (eg. Consumption), but may well be seen as intrusive in others. Time will tell how the user community reacts to the commercialisation of SNS.

Community relevance: *From the Oxford Workshop*, and as previously stated, end-users tend to be suspicious of *IoT*-based services. However, the focus on SNS and participative, dynamic network creation offers opportunities to explore different uses of SNS and online engagement. This may be a way to engage with end-users during the development of services.

9.1.5 SocIoS

Service delivery via SNS

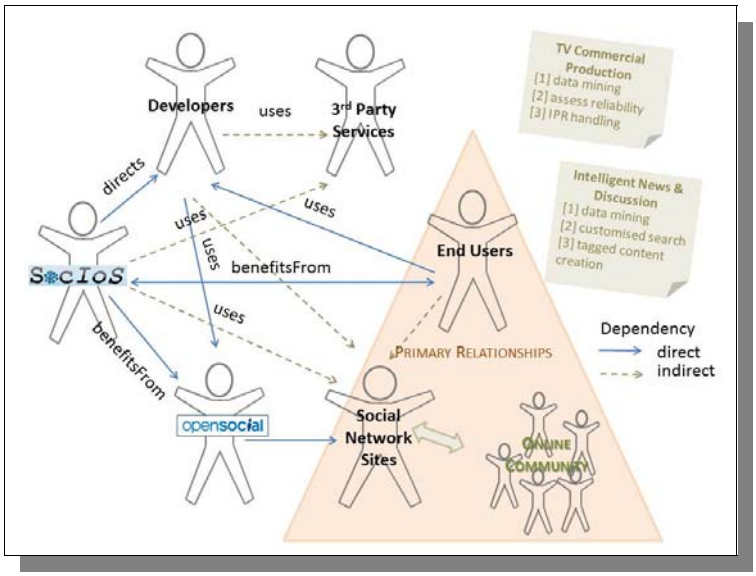
Objective 1.2

Providing a framework to develop services around SNS for commercial exploitation of views and trends expressed by SNS participants.

Website: http://www.sociosproject.eu

FI Importance: Looking at how SNS can be exploited in areas other than originally intended will help shape thinking around what is offered in the FI for participation and online social interaction. It may also indicate that users will not tolerate commercial intrusion into social sites.

Stakeholders:



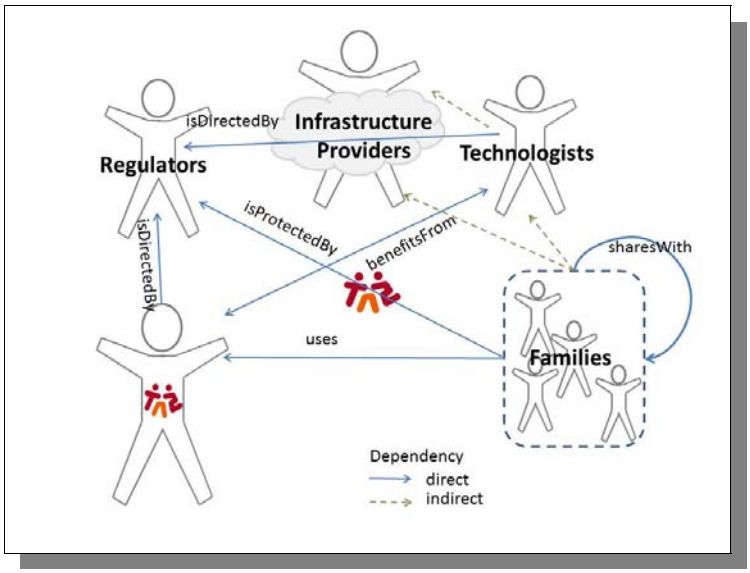
External relevance:	***Digital Agenda***	***Societal Trend(s)***
	DA Columns: 5 and 7 *Opportunity:* This has the potential to add to the understanding of how the community reacts to what the market is offering. This may provide a different mechanism to conduct opinion polls and product trials for a variety of different services. *Risk:* Any commercial incursion into SNS may be treated with mistrust and a reluctance to engage.	The exploitation of what goes on in SNS for commercial gain or purpose may result in some resistance from the online communities who use the SNS. The problem is to describe the work in terms of *Empowerment & Participation*: consumers having their views heard and acted on. This is an opportunity for end-users and content researchers to co-operate if the end-users can see value for them rather than secretive data-mining.
Community relevance:	*From the Oxford workshop*, online communities (SNS) can be seen as an important source of information about the way end-users interact. If issues such as trust and online identity, which were also seen to be significant challenges in the workshop sessions, then this may well be a suitable way to engage directly with consumers within an environment they know and understand whilst addressing concerns about participation.	

9.1.6 TA2 *Interaction Framework* Objective 1.5	Provides technologies in support of social interaction between close-knit groups such as families. The main objective is for sharing and enjoying experiences together even though individual members may be far apart.

Website: http://www.ta2-project.eu

FI Importance: The technologies involved have implications for the infrastructure and how it performs. This is clearly of relevance in considering capacity and performance associated with the FI.

Stakeholders:



External relevance:

Digital Agenda	***Societal Trend(s)***
DA Columns: 5 and 7 *Opportunity:* Exploring aspects of sharing and co-creation in a non-threatening context (ie. between members of the same family) encourages a positive and proactive attitude against isolation and increasing individualisation. It might lead to other informal collaborations among wider communities than a single family.	The TA2 project is all about *Community and Family*. To some degree, it represents the first step in developing fairly sophisticated technology for online dialogue and engagement directed towards a specific goal: this is the next and more dynamic and complete level for SNS-type participation. The technology provides some means for more realistic social

	Risk: encouraging online communication and play between families may increase and exacerbate social isolation and individualism.	engagement, and so it would be easy to predict that it would succeed beyond a single family or group of friends for other uses, which society will determine: it may become a trend amplifier very quickly filling the gap left by the promise of video-conferencing. At the same time, though, without suitable education and support, equally it may increase the growing social inequalities noted in the *Social Impact* studies [43]
Community relevance:	One of the topics for the *Oxford Workshop* was Online Communities, with a finding that it was now time to let the communities themselves take control and direct what they wanted and how they wanted to achieve it. TA2 offers a first step towards building sophisticated technologies around a real world community (i.e. a geographically dispersed family). In time, these same technologies for turn-taking and advanced face and "body" recognition offer significant potential for future online communities to develop more realistic and more intimate online relationships. From the breakout session, though, it is indeed clear that the community needs to be trusted to develop in directions they want and not as dictated by the technology. Interestingly, though and in connection with the *Online Identity* session, with almost complete visual exchange in TA2 (i.e. video as well as audio) identity cannot be protected or hidden in the same way[69].	

[69] It is a moot point whether participants would want to hide or obscure their identities when other family members are involved. However, there may well be cases such as a local community debate where individuals may wish to keep faces and even voices hidden.

9.1.7 WeGOV

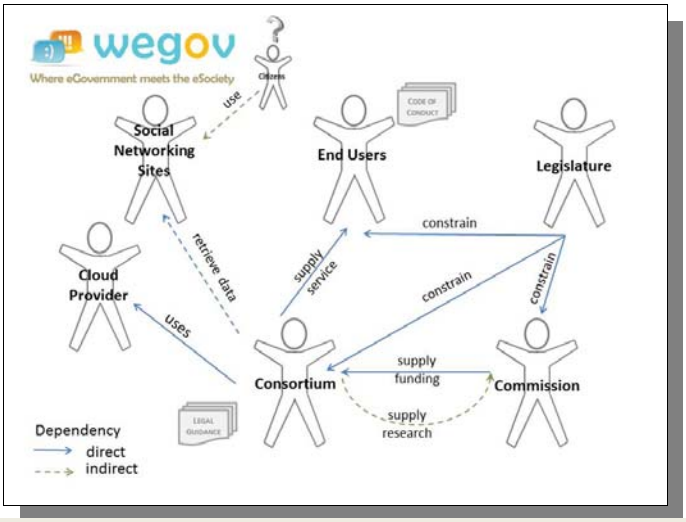
Investigative tooling

Developing tools to support Government agents who wish to seed SNS with items for discussion (such as policy issues). SNS participants may then respond and discuss, their input being aggregated for onward referral to policy-makers, as well as feedback provided from the policy-makers to those who took part.

Website: http://www.wegov-project.eu

FI Importance: Since participation and eDemocracy are clear topics for Digital Europe, exploring how SNS can be used as one possible mechanism for participation will help understand the structures that need to be in place for the FI.

Stakeholders:



External relevance:

Digital Agenda	***Societal Trend(s)***
DA Columns: 3, 6 and 7 *Opportunity:* The importance of SNS over recent years is well known. Seeding discussion in that environment could be of great benefit in engaging citizens with policies before they become set in law, but also develop a sense of trust in democracy as views are shared and feedback given. *Risk:* Taking politics into	*WeGov* is essentially about *Participation and policy making.* There is an opportunity for citizens to become involved with policy making but also to be kept in the loop of discussion and feedback. In addition, though, using SNS as a basis to seed and gather opinion is a real demonstration of society taking technology (SNS) and using it to support and amplify what was already happening but to a lesser extent (MP's surgeries).

SNS may be regarded as intrusive. In addition, opinions expressed may not be representative, but rather be sourced from those who simply want to pronounce (using *WeGov* as a soap box). Issues of trust and privacy may cause additional concerns and impose limitations[47].

Community relevance: *From the Oxford Workshop*, the issues aired in the breakout sessions – identity, security, privacy, online communities – are of direct relevance to the *WeGov* project; additionally, the concerns raised in respect of cloud computing (mainly with regard to data protection) have already had to be dealt with[Error! Bookmark not defined.]. As such, the project would appear to have started at exactly the right time to begin to tackle with practical issues and blockers for the *Digital Agenda* and drives for more government and political participation online. The outcome of the project could well have significant implications for his area in the Future Internet.