Cross-Disciplinary Lessons for the Future Internet

Anne-Marie Oostveen[1], Isis Hjorth[1], Brian Pickering[2], Michael Boniface[2], Eric T. Meyer[1], Cristobal Cobo[1], and Ralph Schroeder[1]

[1] Oxford Internet Institute, University of Oxford, United Kingdom
{anne-marie.oostveen,isis.hjorth,eric.meyer,cristbal.cobo, ralph.schroeder}@oii.ox.ac.uk
[2] University of Southampton IT Innovation, United Kingdom
{jbp,mjb}@it-innovation.soton.ac.uk

Abstract. There are many societal concerns that emerge as a consequence of Future Internet (FI) research and development. A survey identified six key social and economic issues deemed most relevant to European FI projects. During a SESERV-organized workshop, experts in Future Internet technology engaged with social scientists (including economists), policy experts and other stakeholders in analyzing the socio-economic barriers and challenges that affect the Future Internet, and conversely, how the Future Internet will affect society, government, and business. The workshop aimed *to bridge the gap* between those *who study* and *those who build* the Internet. This chapter describes the socio-economic barriers seen by the community itself related to the Future Internet and suggests their resolution, as well as investigating how relevant the EU Digital Agenda is to Future Internet technologists.

Keywords: Future Internet, Socio-Economics, Digital Agenda, Users, SESERV.

1 Introduction

The Internet has become an essential part of the infrastructure of modern life. Relationships are managed online, commerce increasingly takes place online, media content has moved online, television and entertainment are being delivered via the Internet, and policy makers engage the public via programs such as Digital Britain [1], the European Digital Agenda [2], and other worldwide initiatives. Efforts to develop the so-called Future Internet (FI), will either follow as a logical extension of what is in place now, or as something completely different [3].

At the same time the Internet's underlying technology is evolving, it is also changing as a social and economic platform. Yet it is not clear how competing interests should be balanced when technical, societal, economic and regulatory concerns come into conflict. One view is that technology developers should develop innovative technologies with little oversight and regulation so as not to stifle creativity. Social and regulatory concerns can be dealt with as they arise as a result of use. A user-centric view, on the other hand, suggests that any FI must be designed around social and economic concerns, with technology that supports values such as inclusion, privacy, and democracy.

F. Álvarez et al. (Eds.): FIA 2012, LNCS 7281, pp. 42–54, 2012.
© The Author(s). This article is published with open access at SpringerLink.com

Innovation is often serendipitous [4]; for maximum benefit, the complex interactions and even antagonisms between society and technologists need to be nurtured in a suitable and enabling environment. Thus social, legal and technical perspectives inevitably intertwine. Understanding the interactions between technologists, society, legislation and regulation is therefore indispensable in shaping the Future Internet and associated applications and services [5, 6]. In this chapter we investigate the societal aspects of the FI as seen by social scientists, policy makers and technologists involved in the central European Commission-funded projects designing these technologies.

How the Internet pervades our professional, commercial, political and leisure activities is an important question for Europe and beyond. Boosting EU R&D efforts is a key element of the *Digital Agenda* for Europe [2]. EU-funded research aims to make the Internet of the future a dynamic place for innovation, growth and jobs. The European Commission is currently reviewing the progress of some 140 "Future Internet" research projects which it supports. Given the relevance of planned Digital Agenda actions for the SESERV workshop's participants and their proximity to several themes included in the programme, it seemed important to learn how familiar with this EU instrument they are and the value it provides to their current activities. Therefore ten participants were interviewed on this topic.

The specific socio-economic topics discussed during the workshop 'The Future Internet: The Social Nature of Technical Choices' organized by the SESERV consortium[1] were based on the results of an online survey across the FI community. The structure of this chapter is as follows: in Section 2 we discuss the socio-economic topics that emerged via representatives of FI projects as they relate to any barriers they face in their development work. From such discussions, eight cross-cutting strategies emerged that provide potential resolutions to these socio-economic challenges (Section 3). Finally, in Section 4 we identify how relevant the Digital Agenda is to Future Internet technologists and examine its value for the projects interviewed.

2 Societal Concerns and Challenges

In 2010, the Internet Society defined an 'Internet Ecosystem' [7], with stakeholders from a traditional infrastructure perspective. In recent years, however, the rapid convergence of technologies has increased the scope of stakeholder engagement beyond what was originally described. The European FI initiative has led developments both within the core ICT programme and the Future Internet Public Private Partnership (FI-PPP) initiative[2]. A significant increase in the diversity of roles is seen, along with an increased emphasis on users in addition to infrastructure and a blurring of roles between major market players [8]. The concerns of the Internet have moved from structures for the delivery of data, to socio-economic structures supporting information and knowledge exchange.

Many societal concerns emerge as a consequence of FI research and development. Relating these specifically to the FI ecosystem rather than to more general societal

[1] SESERV (Socio-Economic Services for European Research Projects). See `http://www.seserv.org`

[2] The Future Internet – Public Private Partnership, `http://www.fi-ppp.eu/`

issues is essential FI technology projects in debate. Content analysis of two recent reports, *Social Impact of ICT Studies* [9] and *Towards a Future Internet* [10] identified 16 societal concerns for the FI that raise significant technical, commercial and regulatory challenges: (1) Regulation; (2) Privacy; (3) Online Identity; (4) Green Issues; (5) Security of Communications; (6) Content Regulation; (7) Cloud Computing; (8) Trust; (9) e-Democracy; (10) Digital Citizenship; (11) Digital Inclusion; (12) Online Communities; (13) Internet of Things; (14) Consumers and Suppliers; (15) Distributed Knowledge; (16) Cybercrime and Cyberlaw.

Representatives from FP7 Future Internet projects (n=98) rated the relevance of these socio-economic topics for their projects on a subjective scale from "Not Relevant" through to "Absolutely relevant, a key issue" in an online survey. The following six issues were of most interest: *Privacy and Data Protection* including user data, file-sharing control, selling of personal information; *Online Identity* including anonymity, digital presence, rights to delete information; *Security of Communications* including legal implications*; Online Communities* including social networks, virtual relationships; *Internet of Things* and the connections between people and devices; and *Cloud Computing* including the risks and benefits of virtual access to information. Some topics (Green Internet and Cybercrime, as well as Digital Inclusion) were disregarded by all projects, while applied to only a few [11].

During a workshop and seminar held at the University of Oxford in June 2011, experts in FI technology engaged with researchers such as social scientists (including economists), policy experts and other stakeholders to explore the socio-economic aspects of the FI, and conversely how the FI will affect society, government, and business [12]. Special break-out sessions on each of the six key issues were organized to facilitate a more focused discussion between the 69 participants, with the societal concerns and challenges from these 1.5 hour break-out sessions discussed below.

2.1 Privacy and Data Protection

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 [13]. Careers and personal lives can be severely affected by not considering what information (including multimedia – photos, videos etc.) is disclosed online. For most users, the main concern is the extent to which information was becoming public, and some are now allowing less of their content to be published openly. This change in general awareness will make FI applications safer (e.g., customers and regulators will demand that location-aware services protect user privacy). But while attitudes towards privacy are changing significantly, for many the level of privacy concern is decreasing.

Privacy is heavily compromised by a lack of awareness as much as by technical or cost issues. Users supply personal information to service providers with every post, query or click in applications like Google Search, Facebook, and Twitter. Users benefit from this data exchange because they can use search technology, social networks and the like without charge. Yet the relationship between citizens and service providers is highly asymmetric, and the resulting loss of privacy for users and bystanders is profound. The providers of these services exploit this content in a wide variety of ways: to attract a larger audience share; to classify users based on their

personal data to 'improve' the service; to classify and index data (including personal relationship data) which allows the service to be further enhanced; to create personalized advertising; and to provide information to businesses and governments, for payment and/or to meet legal obligations.

The most successful Social Network Sites or online retailers are now among the largest and most profitable businesses, and yet typically accept no responsibility for user-generated content[3]. Users can publish sensitive, sometimes scandalous information about third parties, which is propagated freely by the service provider. The victims have few protections and very limited recourse. They can ask the service provider to remove the offending content after the fact, or sue the user who posted it (if the service provider reveals their real identity, and that user falls under a jurisdiction to which the victim has access).

The trend is towards an increase in asymmetry as service providers improve exploitation and find new opportunities to capture personal data. Personal data is increasingly available to the service provider and to other users, commercial customers and government agencies. The risks from widespread disclosure - should the provider be hacked or forced by government agencies to release information - are acute. European privacy regulations provide little protection due to technical and jurisdictional limitations; European service providers may therefore find it harder to compete.

Privacy clearly goes hand-in-hand with issues of security and trust. Therefore, one could expect appropriate technical and procedural protection in support of users online. To some degree, users may have unrealistic expectations of technical provision for privacy. However, it is equally true that users themselves should be able to make appropriate judgments about suitable protection and data management. Thus, examining how users behave and *wish* to behave may help determine requirements.

2.2 Online Identity

Online identity is inextricably related to issues of data, privacy and rights (including, though not limited to, digital rights). 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. It thus becomes necessary to examine the relationships between all data and identity.

Identity is not easy to define, and current definitions diverge. Common baselines and vocabularies are needed to enable a multidisciplinary discussion of identity. Society conceives identity as stable: identity in terms such as surname and passport and the like is assumed stable by policy-makers and in terms of social norms. Yet, in scholarly discourses and research on identity, it is often characterized as inherently dynamic (changing over time and context). In addition, individuals might very well experience their identity as fluid or develop multiple identities [14]. This clash between these two opposing stances is not sufficiently addressed.

A number of socio-technical challenges arise. First, there is a need to develop tools for managing online identity. As applications are increasingly tied to each other, users need assistance in understanding the implications of these connections for the sharing of their data and identity/-ies. Designing tools that enable multi-scale filtering of

[3] Though this is not always the case, e.g. Italian law puts the onus on the service provider.

content by users (e.g. more control of what information is accessible to whom) is an immediate challenge to be addressed.

Second, in an online/networked environment, users leave digital footprints. These data can be misused by third parties. In addition, more sophisticated methods for analyzing large-scale data from, for example, archived system logs, mobile phone usage, and other online interactions make it possible to identify individuals based on their preferences, patterns and social networks. Sometimes it's justified (mobile phone usage for billing), but generally anonymization is desirable. This places an increased onus on developers, legislators, third parties and researchers to disclose the degree to which data reveal identity.

Third, currently anonymity cannot be guaranteed online and individual users can, with some effort, almost always be identified. Users need to know the levels of anonymity possible. This leads on to the question whether anonymity should form part of a more general set of digital rights. One challenge then is to develop features that allow for increasing levels of transparency: end-users could be made aware of the level, or lack of, anonymity that systems allow for.

Finally, the right of an individual 'to be forgotten' poses specific problems. This relates directly to the interplay between an individual's rights and those of the community. Are there occasions so significant or horrific an individual's identity online should *not* be protected, in the interests of the common good?

2.3 Security of Communications

Security of communications is not about privacy or identity management. Instead, it is about managing the risks to the smooth functioning of 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 vast resources, clouds raise concerns about the risks they pose. For instance, what if cloud providers or their customers were malicious? If we cannot protect the data, how can we guarantee that the services can be protected? Who should be responsible for meeting the security threats of clouds: the operator, developer or customer, or even the regulator? One extreme scenario could be that the cloud provider becomes the key party responsible for the cloud with worrying implications for the degree of freedom of users. In contrast, little or no regulation could be a risk to parts of the innovation, as a deterrent to creative FI services. And any legislation needs to be cross-jurisdictional.

Even when compliant to existing EU legislation concerning storage and privacy, the nature of the cloud brings new risks. Many SMEs are thinking of moving their regular ICT needs into a cloud and for a smaller company, it could be better *not* to impose regulation, especially if it lags behind innovations. Service providers could be compelled to manage the risks, and customers need to trust the infrastructure provider. But over-monitoring may make users distrust the service.

Security can be addressed via technical requirements, but the more difficult emerging challenges are socio-economic: what are the obligations of those who did not expect to be supporting these services? Access to risk expertise and managing risk are essential. A cloud provider has a team of security analysts or information security analysts, and large

corporations employ legal services firms. Others, however, may not have access to risk experts or be able to cope with security threats. Most medium and small scale companies cannot afford to hire technical risk analysts, lawyers and other experts. Similarly, domestic users will have to trust the information provided. Security could be left to the market, with customers avoiding services that they find too risky. But the *laissez-faire* of a completely free market is not enough to manage security risks. There is a need for regulation, and one simple approach could be to force cloud service providers to publish statistics about the health of their activities and their monthly attacks, allowing for validation. Yet information about security is also very sensitive, which means that service providers might not be willing to reveal these data. Hence there is a need for transparent metrics for comparing 'trustworthiness' and auditing standards to ensure that what service providers publish is credible.

2.4 Internet of Things

Definitions of the Internet of Things (IoT) vary. At a minimum, the IoT can be thought of as including all manner of mobile devices, including telephones, PDAs and sensors equipped with intelligent and large-scale data analytics. The key ingredient is the seamless interaction between different systems: IoT technologies are bringing data together to create new services. The promise of the IoT is to use online technology combined with sensors which might automate the surveillance and management of the more mundane aspects of life (food purchases which are linked to fridge monitors; automation in the home; and so forth).

Many barriers have been identified for the adoption of the IoT within the FI ecosystem. First, participants indicated that current definitions are too abstract and hard to grasp, too academic without enough focus on design and applications. This is partly due to the lack of interaction between the actors in the design and application domains. Currently, development is characterized by 'doing' rather than by reflexivity and deliberations about design. Even so the general public perceives the IoT in terms of Big Brother: 'Smart' applications tend to be received with skepticism by the general public, such as the 'smart' bins in London provided with sensors which were quickly labelled 'spy'-bins [15]. In popular discourse, technologies are described as intelligent autonomous agents 'affecting' a passive public. Changing this attitude and the underlying technologically deterministic view would help to inform design.

IoT technologies are predominantly designed for domestic purposes, such as the interactive 'intelligent' Internet fridge. Applications need introduction in existing infrastructures such as transport and health systems to make them more intelligent. Additional challenges are the vast amounts of data generated. Individual systems, however, are not able to harness the data and so we need an 'intermediate' level of technology[4]. Further, where are boundaries between public and private data? One example is the 'passive' monitoring phones: with mobiles on, users can be tracked at all times. As well as transparency, the advantages and disadvantages (e.g. spam risks) need to be weighed up. Users could, for example, be presented with different levels of

[4] Possibly by extending *senslets*, `http://www.inets.rwth-aachen.de/fileadmin/templates/images/PublicationPdfs/2008/Senslet_EuroSSC.pdf`

'sign-off' options to balance against the possibility of generating moral panics by greater awareness. It is also vital to provide opportunities for 'offline' access to services; 'opting out' currently unacceptably penalizes people.

Finally, as ever, there may be unintended consequences. 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 see human expertise replaced by automated sensors. Such effects are important.

2.5 Online Communities

Social media have grown rapidly – today nearly 4 out of 5 active internet users visit social networks and blogs [16]; 20% of online time is spent on social networking sites (SNS's), up from 6% in 2007. SNS's reach 82% of the world's online population [17]. Online communities center on how users interact with and exploit the range of social networking applications (e.g., government, leisure and work). A critical success factor is to maximize activity, mainly achieved irrespective of the purpose of communications. However, it is also necessary to comply with required data protection legislation in relation to responsibilities and individual actions (e.g. consent). Herein lies a contradiction: Privacy compliance, often promoted as a means to increase trust and hence participation, can also act as an inhibiter to greater activity. Individuals use SNS's because their perception of risk is considered low enough, whilst developing an appetite for risk, upping participation regardless 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 - if it is desirable to monitor and mine data - without violating a citizen's right to privacy. It is unlikely that the successful paradigms of the last decade, social networking and clouds, would have prospered if they'd been subject to the European regulatory environment from the start. The try-it-and-see approach has led to a balance over time: participants have explored their preferences iteratively. Social networking has in fact been a large experiment in people's appetite for privacy.

Online Communities highlight the basic dichotomy: is it technology or society which shapes the ICT future? The answer for now at least is that 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. The focus would move towards societal behaviours and away from technology, and require appropriately skilled cross-disciplinary researchers with an understanding of these communities and what makes healthy and vibrant online communities.

Elsewhere, SNS content (especially user profiles) are being synchronized live across networks. What does this do for user control and user-centeredness? User-centric platform-bridging applications with transparent filtering options can be developed, so users should be able to manage and control sharing easily with the online communities. Better tools in general are needed for managing online communities such as smaller community hubs that mirror the cognitive limit for social relationships. There are both limitations and strengths to smaller online

communities: there is less information accessible but smaller communities could be one way of handling privacy issues and the right to be forgotten (see above) in line with community benefit.

Finally, users make innovative and creative use of systems and applications in the development of online communities. Technologies are not the only drivers in the development of new types of online communities where different structures may be required for sharing or co-creating content. There is a need to balance bottom-up and top-down technology development, and to involve members of the communities.

2.6 Cloud Computing

Just as energy production benefits from economies of scale when consumers transfer responsibility to an electrical grid for centralized production, so do those needing ICT resources benefit from exploiting cloud facilities. Europe could gain significantly from the resulting new business opportunities even though it lags behind the rest of the world with clouds, not least because much of European enterprise is SME based for whom investment in large and under-used ICT equipment may not be economic. Early end-user engagement is critical to direct investment and design. At the same time, of course, issues of trust and security cannot be overlooked and these need to be tackled alongside interoperability and portability.

There are a number of barriers to the adoption of cloud computing within the FI ecosystem, such as the lack of a global legal framework. The global nature of cloud computing requires consistency in laws across jurisdictions (e.g. to notify data access breaches). International coordination is important here but also bottom-up feedback from users. Definitions also pose problems with clouds: are they infrastructure or do they encompass nearly all online activity? Another barrier is that EU discourse focuses on risks and less on benefits, especially economic ones, and is slow to adopt new technology, sticking for instance with grids instead.

User concerns relate largely to control. There is a need for more transparency and control. Contracts vary greatly between different providers and often do not allow user control over where their data is stored; many companies run services on a third company's cloud infrastructure; end-users don't deal directly with the cloud provider and yet rely upon them to secure the data and provide the actual service. Security in general is a concern, though is tightly coupled with transparency. Designing for interoperability and portability while allowing customization is also of concern. Portability will allow users to move from one cloud provider to another and avoid platform lock-in. Finally, providers might gain a large amount of meta-data about the activities, locations, and contents of user interactions with their services; again transparency would be appreciated.

3 Cross-Cutting Resolutions to Socio-Economic Challenges

The discussions in Section 2 yielded recurring strategies which suggest eight cross-cutting resolutions to the socio-economic challenges identified.

3.1 Call for Increased Transparency

A dominant trend across discussions was a call for increased transparency on all levels for end-users of networked ICTs. Systems and applications should offer end-users tools that allow end-users to know exactly who has access to the contents of their online activities. Advanced transparent filtering options are becoming increasingly critical as more and more online networks are being synchronized, as are tools that assist users to manage the various communities.

Transparency also relates to ISPs and data storage, particularly with cloud-based services. To make security risks more transparent for end-users, providers might publish monthly statistics on attacks. End-users should be able to easily identify where and how their data is stored and is or will be used.

3.2 Call for More User-Centricity and Control

Discussions converged on a call for more user-centricity and control: increased user-centricity in the design of applications. Users could be allowed some means of influencing applications/systems on an ongoing basis; creative uses could feed back into systems to improve them and innovate further. Control is particularly evident in the context of opt-out options with more granularity required. Additionally, a range of different choices for how user data is stored could be offered (e.g. location). Finally, users need to assess and control their security risks and risk management.

3.3 Continuing Need for Further Multi-disciplinary Bridging

Without exception the discussions called for increase cooperation across sectors. While it is easy to call for knowledge-exchange, dialogue and collaboration across and beyond academic fields, industry, developers, designers and users gaps exist between privacy researchers and IoT engineers, or between eHealth practitioners and IT suppliers, for instance. Creating frameworks for knowledge exchange between users, developers, regulators and researchers would facilitate connection between technical and legal analysts and a better understanding of risks could avoid ‘siloization’ or ‘pillarization’. The expertise of different communities should be included in *all* stages of technology development and design via multi-disciplinary engagement and institutions.

3.4 Striking a Balance between Extremes in Debates and Design

A cross-cutting theme that emerged across several discussions (Online Identity and Communities, the IoT, and Privacy) was a call for more balanced approaches in design avoiding dichotomized thinking. For example, there is a need for a balance between identity as singular and stable (e.g. passport) as well as completely fluid and dynamic. How identity is perceived has a consequence for system design such as more nuanced views and multi-disciplinary insights, like an identity continuum from stable to dynamic. Similarly, design needs to balance bottom-up and top-down

innovation: new forms of communities are potential drivers of technology development. Elsewhere, eHealth privacy practices and perceptions suggest another balance to strike: a middle ground that allows proportionate access to patient records rather than either a *laissez-faire* approach or over-regulation would be beneficial. Finally, discourses on privacy tend to lack balance between risk and opportunity: the IoT technologies, are often perceived as 'big brother' surveillance, for instance.

3.5 Facilitating the Development of Digital Literacy

The need for greater digital and media literacy education was expressed across sessions (Security, Privacy, Identity and Online Communities) the core concerns being user ability to critically manage privacy and identity. Arguably, digital literacy skills can equip users with more sophisticated tools for managing and understanding identity and thus solve some of the problems encountered with privacy. Security risks could be managed better with best practice guidelines and more awareness. This highlights non-technical social challenges that need to be addressed alongside the design and development of socio-technical systems.

3.6 Addressing the Lack of Common Vocabularies and Definitions

Common vocabularies and better definitions (Identity; Internet of Things; Online Communities; Cloud Computing) have the potential to be enablers: in cloud computing current definitions diverge between infrastructure and all online activities. For the IoT definitions are too academic, lack focus on design, and difficult to apply in technology development. For identity, there is a need for definitions that acknowledge a close link with questions of privacy, data and rights in digital contexts. Common vocabularies could benefit new technologies and their adoption. For now, they are missing, in the case of the multi-device IoT. Likewise, a more advanced vocabulary is needed to describe the maintenance, structure, and scales of online communities. Seen in light of multi-disciplinary bridging and collaboration, there is a need for adequate vocabulary and definitions that can be applied across sectors and contexts.

3.7 Need for Clarity about Digital Rights and Digital Choice

Some discussions (Privacy, Internet of Things and Online Communities) agreed on the need to clarify digital rights and digital choices: what levels of anonymity should be granted, to whom and in what context? In the case of eHealth, for example, there is a need to balance an individual's right to anonymity against appropriate access to detect and tackle emerging health issues. Another question concerns the right to be forgotten: to have information deleted. As stated, this might not apply to content of historic or humanitarian value. Digital choice can be exemplified in relation to the IoT, where off-line alternatives should be available.

3.8 Enabling Global Regulatory Frameworks

Global regulatory frameworks are particularly pertinent (Security, Online Communities and Cloud Computing). Suggestions here include consistency across jurisdictions for data breaches as well as for anonymity. Increased trans-national legislation could ensure that providers are not discouraged from operating in certain countries (e.g. where providers are liable for users' IP infringements).

4 The Future Internet Community and the Digital Agenda

ICT is regarded as increasingly critical for the future growth and development of Europe. *Europe 2020* [18] together with the *Digital Agenda* [2] outlines the main challenges and opportunities over the coming decade including for the FI. The overall aim of the Digital Agenda is to "deliver sustainable and social benefits from a digital single market based on fast and ultra-fast internet and interoperable applications".

At its center is an assumption about the mutual reinforcement between innovation in the ICT sector and consumption which, in turn drives technological improvement. This *virtuous cycle* runs something like this: if there are attractive services and content available online across all member states this will motivate increased demand. More users will want access, and look for more and improved content and services. Increased demand in turn provides the necessary financial basis for improvements in the supporting infrastructure. This investment enables ever more sophisticated service and content generation and support, and so on.

Against this background, the Digital Agenda recognizes some seven major challenges or *obstacles*: 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, which relate principally to infrastructure and commerce; and the *virtuous cycle* must address these obstacles.

The previous sections have highlighted that the FI is of interest to different stakeholders, and particularly the role of *users* in terms of improving technology design and alleviating fears around privacy and security risks. These social aspects should not be down-played in the Digital Agenda. The focus on infrastructure and cross-border eCommerce fails to give a central place to end-users. The assumption of the *virtuous cycle* is that end-users will participate. If so, considerable effort needs to be invested in understanding the *use* of services and the inhibitors to online activity.

The Digital Agenda needs to engage closely with the FI community. Knowledge of the aims and relevance of the Digital Agenda is highly variable across European ICT projects and actors. A number of informal interviews with participants in this community were conducted, and while perhaps not representative, clearly the projects had little widespread understanding of the Digital Agenda's aims. If familiar at all, it was seen as irrelevant to the specific concerns within the projects themselves. Europe may set an agenda and provide motivation for technology advance, but its relevance and meaning for projects is unclear. Some believe the EU should not seek to micro-manage projects: if innovation is to deliver, a large amount of autonomy is required. Especially in discussions of the *Internet of Things,* designers and business developers view the Digital Agenda as a restriction on new business plans and technology designs. This also affects global competitiveness. Even so, there was a general

consensus that the Digital Agenda is central to taking Europe forward technologically as well as socially: though too high-level lacking global relevance beyond the EU, as an instrument for future strategy, technologists and social scientists have much to contribute to the Digital Agenda and *vice versa*.

5 Conclusions

This chapter has presented the views of social scientists and technologists working on the FI. The community has developed possible future strategies and priorities. The results represent a snapshot of the challenges facing those undertaking FI research. There is no doubt that the FI ecosystem is an increasingly rich, diverse and complex environment, and Challenge 1 projects are aware of societal concerns and challenges, and of their potential resolution. In contrast, the Digital Agenda is not well understood by technologists and there is a gap between a set of high level policies and incentives that are particularly focused on infrastructure and complex regulatory processes as against the users of the technologies being developed. Regulations currently ignore some of the concerns of citizens and there is a disconnect between the 'stakeholders' of the FI and the Digital Agenda. The European Commission needs to find a way to update the Digital Agenda in response to the needs of a broad spectrum of people and communities rather than focusing only on big companies or governments. For instance, rural and remote regions, non-organized communities and even SMEs seem to be under-represented in this policy aimed at 2020: different 'soft' design mechanisms may help the Digital Agenda to adapt to the social, political, educational, labour, and environmental needs of the community. If the Digital Agenda is not embedded in the principles of openness, adaptability, participation and transparency, it is hard to see how it will succeed. Supporting technologists in their understanding of the potential broader impacts of the FI and its adoption through dialogue with social scientists must be central to this effort. To realize the benefits for the widest possible range of stakeholders, there will need to be increasing engagement between those who study and those who are building the Future Internet.

Acknowledgements. The SESERV project (FP7-2010-ICT-258138-CSA) is funded by the European Commission. The authors would like to thank all participants to the Oxford scientific workshop and especially Ben Bashford, Ian Brown, Tony Fish, Sandra Gonzalez-Bailon, Christopher Millard and Mike Surridge for facilitating.

Open Access. This article is distributed under the terms of the Creative Commons Attribution Noncommercial License which permits any noncommercial use, distribution, and reproduction in any medium, provided the original author(s) and source are credited.

References

1. Mandelson, P., Bradshaw, B.: Digital Britain: Final Report. Department for Business Innovation & Skills and Department for Culture, Media and Sport (2009), http://www.official-documents.gov.uk/document/cm76/7650/7650.pdf
2. European Commission: A Digital Agenda for Europe. European Commission (2010), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:REV1:EN:HTML

3. The Internet Society: How is the Internet evolving? (2011), http://www.Internetsociety.org/internet/how-it's-evolving/future-scenarios
4. SESERV: The Future Internet Debate: Will the Design of the Future Internet be Driven by Technology or Societal Concerns? (2011), http://www.seserv.org/panel/conferences-webcasts#debate
5. Callon, M.: Society in the Making: The Study of Technology as a Tool for Social Analysis. In: Bijker, W.E., Hughes, T.P., Pinch, T. (eds.) The Social Construction of Technological Systems, pp. 83–103. The MIT Press, Cambridge (1987)
6. Hausheer, D., et al.: Future Internet Socio-Economics – Challenges and Perspectives (2009), http://www.future-internet.eu/fileadmin/documents/madrid_documents/FISE/FISE_position_paper_final.pdf
7. The Internet Society: The Internet Ecosystem (2010), http://www.isoc.org/pubpolpillar/docs/internetmodel.pdf
8. Boniface, M., et al.: First Report on Economic Future Internet Coordination Activities. SESERV Deliverable D2.1, Socio-Economic Services for European Research Projects FP7-2010-ICT-258138-CSA (2011)
9. Universitat Siegen: Final Report on the Social Impact of ICTs in Europe to the European Commission, SMART No2007/0068. European Commission (2010), http://ec.europa.eu/information_society/eeurope/i2010/docs/eda/social_impact_of_ict.pdf
10. Blackman, C., et al.: Towards a Future Internet: Interrelation between Technological, Social and Economic Trends. European Commission (2010), http://www.internetfutures.eu/wp-content/uploads/2010/11/TAFI-Final-Report.pdf
11. Boniface, M., et al.: Initial SESERV Survey Results, Challenge 1 Projects: Socio-Economic Priorities. SESERV (2011), http://www.seserv.org/fise-conversation/socio-economicpriorities/SESERV-Survey-Results_May11.pdf
12. Oostveen, A.-M., et al.: First Year Report on Scientific Workshop. SESERV Deliverable D1.2, Socio-Economic Services for European Research Projects FP7-2010-ICT-258138-CSA (2011)
13. Pötzsch, S.: Privacy Awareness: A Means to Solve the Privacy Paradox? In: Matyáš, V., Fischer-Hübner, S., Cvrček, D., Švenda, P. (eds.) The Future of Identity. IFIP AICT, vol. 298, pp. 226–236. Springer, Heidelberg (2009)
14. Jones, S.R., McEwen, M.K.: A conceptual model of multiple dimensions of identity. J. Coll. Student Dev. 41, 405–414 (2000)
15. Harris, E.: Smart wheelie bins to charge for waste. The London Evening Standard, London (2007)
16. Nielsen: State of the Media: The Social Media Report Q3 2011 (2011), http://blog.nielsen.com/nielsenwire/social/
17. Radwanik, S., et al.: It's a Social World: Top 10 Need-to-Knows About Social Networking and Where It's Headed (2011), http://www.comscore.com/Press_Events/Presentations_Whitepapers/2011/it_is_a_social_world_top_10_need-to-knows_about_social_networking
18. European Commission: Europe 2020: A strategy for smart, sustainable and inclusive growth. European Commission (2010), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:2020:FIN:EN:PDF