WORKING
PAPER

The Future of the Internet Economy

A Discussion Paper on Critical Issues

CONSTANTIJN VAN ORANJE-NASSAU
JOACHIM KRAPELS
MAARTEN BOTTERMAN
JONATHAN CAVE

WR-548-EZ

December 2009

Prepared for The Netherlands Ministry of Economic Affairs

This product is part of the RAND Europe working paper series. RAND working papers are intended to share researchers' latest findings and to solicit informal peer review. They have been approved for circulation by RAND Europe but have not been formally edited or peer reviewed. Unless otherwise indicated, working papers can be quoted and cited without permission of the author, provided the source is clearly referred to as a working paper. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.
RAND® is a registered trademark.

EUROPE

Preface

The Dutch Ministry of Economic Affairs asked RAND Europe to explore the critical issues arising from the emerging Internet economy, in order to inform Dutch policy makers and to help prepare for the Dutch position in the Organisation for Economic Co-operation and Development (OECD) conference on the Internet in 2008. This document is a result of that exploration. It is based on a horizon scan of literature and subsequent discussion in four thematic seminars organised with two distinct groups of experts on 17 and 18 October 2007. The ideas and views of the experts form the main content of the paper. However, these are supported and complemented by findings from the horizon scan and ongoing RAND studies to ensure coverage of the broad range of topics addressed by the OECD Ministerial Conference.

The purpose of this document is to provide a basis for a continuous exchange of ideas relevant for current and future policy making in response to the challenges posed by the emerging Internet economy. It addresses emerging trends and underlying values and the possible role of governments in dealing with the unfolding Internet economy.

Besides being a discussion paper, this document also serves as a briefing paper for the Dutch delegation to the 2008 OECD Ministerial Conference. For this reason it has been decided to attach – in Appendix A - a deeper exploration of the four main themes of the OECD Ministerial Conference; even though elements overlap various themes, and some themes have led to more insightful exchanges of views than others. As the OECD Agenda has evolved since the expert seminars, the paper will not be fully aligned with it. However, the authors have endeavoured to restructure the content to mirror as much as possible this OECD Agenda as it stood at the end of December 2007.

This paper is not a policy document. The opinions expressed by the authors do not necessarily reflect the position of the Dutch Ministry of Economic Affairs. For further information please contact:

Constantijn van Oranje
RAND Europe
Westbrook Centre
Milton Road
Cambridge CB4 1YG, UK
Tel: +44 1223 353329
Email: oranje@rand.org

Acknowledgments

This paper relies heavily on the contributions of external experts to the email based consultation and the expert seminars, which were held in Scheveningen, The Netherlands, on 17 and 18 October under the auspices of the Dutch Ministry of Economic Affairs. The project team acknowledges their invaluable contributions to the spirited exchange of ideas on the future of the Internet economy (names listed in Appendix D – List of Experts).

We also acknowledge the constructive role of the Ministry of Economic Affairs and its open and innovative approach, involving internal and external experts, analysts, researchers and graphic designers to capture the relevant concepts of the evolving Internet economy in words and images. We thank the project team of the ministry for its positive contribution.

Finally the team wishes to acknowledge substantive contributions made on international governance and Internet self-regulation by Mr Chris Marsden of the University of Essex.

Glossary

Term – Acronyms	Explanation
CCTV	Closed Circuit Television
CERN	European Organisation for Nuclear Research
CONGO	Conference of Non-Governmental Organisations
CPU	Central Processing Unit
DNS	Domain Name System
DRM	Digital Rights Management
ECOSOC	Economic and Social Council of the United Nations
GÉANT	Main European multi-gigabit research and education network
GPL	General Public License
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information, Communications Technology
ID	Identity
IP	Internet Protocol
IPR	Intellectual Property Rights
IPv6	Internet Protocol version 6
ISP	Internet Service Provider
ISPA	Internet Service Provider Association
MMORPG	Massively Multiplayer Online Role Playing Games
OECD	Organisation for Economic Co-operation and Development
PSTN	Public Switched Telephone Network
RFID	Radio Frequency Identification
RTD	Research and Technological Development
SIS II	Next Generation Schengen Information System

SME	Small and Medium sized Enterprise
UCC	User Created Content
VoIP	Voice over Internet Protocol
WGIG	Working Group on Internet Governance
WWW	World Wide Web

Contents

Preface iii
Acknowledgments v
Glossary vii
Executive summary 11

CHAPTER 1 **Introduction 15**

CHAPTER 2 **Emerging trends: Intensity of globally changing interactions and trade offs 19**
2.1 Globalisation trends: Universal connectivity and access, and the cost and benefits of diversity 19
2.2 People trends: Being led by our kids and the empowerment of the individual 22
2.3 Technology trends: a new era of pervasive computing creating intelligent environments 25
2.4 Relevant security trends: Accepting risks, increasing transparency and taking precautions as in the physical world 26
2.5 Relevant economic trends: Balancing collaboration and competition, stability and innovation 28
2.6 Governance trends: accepting the global, multi facetted nature of the Internet and dealing with failing jurisdictions and poor enforcement 31

CHAPTER 3 **Emerging values: Redefining how people and organisations interact 35**
3.1 To know and be known 35
3.2 Awareness and trust 36
3.3 Accountability and the power of the collective 37
3.4 Accepting Diversity 37

CHAPTER 4 **The changing role of government; between idleness and engagement 39**
4.1 Public goods for all 39
4.2 Dealing with virtual worlds 40
4.3 Governing the ungoverned 40
4.4 Between collaboration and competition, supporting innovation 41

CHAPTER 5 **Concluding Remarks** **43**

APPENDICES **45**

Appendix A: Thematic discussion: delivering a strong message at the OECD Ministerial Conference **47**

Theme 1, Infrastructure: Facilitate the convergence of networks and devices, applications and services 47

Theme 2: Socio-economic dimension: Fostering creativity in the way we connect, work, make money and live. 51

Theme 3: Reliable use and common Trust: strengthening confidence and security 58

Theme 4: Internet Governance: ensure that the Internet economy is truly global 64

Appendix B: Reference Bibliography **71**

Appendix C: Methodology **77**

Appendix D: List of Experts **81**

Executive summary

RAND Europe conducted a horizon scan of literature to relating the main topics identified by the Organisation for Economic Co-operation and Development (OECD) as agenda items for the 2008 Ministerial Conference on the Future of the Internet. This scan produced a list of topics, which was sent to selected national and international experts for ranking and comments. The message to policy makers that broadly emerged from the expert consultation can be summarised as:

> *Keep the Internet available and open, by ensuring safe access and use - primarily by 'light touch' measures aimed at raising awareness rather than coercive intervention; and by embracing the Better Regulation principles of minimal, flexible and accountable regulation through appropriate self- and co-regulation, with special attention to issues of participation, transparency, compliance and control of spill-over (e.g. market distortions). Any residual adverse socio-political fallout should be dealt with through 'traditional' public policy measures.*

The result of two rounds of expert consultation was a prioritised set of issues which were explored further in four half-day seminars, each addressing one of the four themes of the OECD Agenda. Participants were challenged in a moderated discussion to expand on the topics; assessing their relevance from the perspectives of citizens, governments and business. Subsequently, they were asked to discuss the driving trends and possible underlying issues - loosely labelled as 'values' - which policymakers would need to take into account. Finally, options for government intervention were discussed.

During the study six trends were identified, each consisting of a number of sub-trends. These are:

1. Globalisation trends: Universal connectivity and access, and the cost and benefits of diversity;
2. People trends: Being led by our kids and the empowerment of the individual;
3. Technology trends: a new era of pervasive computing, creating intelligent environments;
4. Relevant security trends: Accepting risks, increasing transparency and taking precautions just like in the physical world;
5. Relevant economic trends: Balancing collaboration and competition, stability and innovation;

6. Governance trends: accepting the global, multi-faceted nature of the Internet and dealing with failing jurisdictions and poor enforcement.

From the trends and the responses that these trigger, a set of emerging (non-exclusive) 'values' were identified:

Identity and privacy

- Control over personal data: people do not own personal data, yet should be in a position to control it;
- Privacy: the use of private personal data must be sufficiently justified; people want to be protected and not spied on;
- Anonymity: people have the right to keep secrets, and possibly even the right to certain anonymity;
- Multiple identities: people's identities consist of different elements and they want to retain control over them;

Transparency and openness

- Transparency: people require transparency to enable them to decide about the desirable level of privacy and what level of risk they will take;
- Responsibility: people and organisations need to define how responsibility is allocated and assumed, and how accountability is established;
- Sharing, openness, and fairness: people self-organise and private and public organisations will facilitate this as they are aware that a lot more can be achieved and many more people can be engaged by opening up processes and information and inviting active participation.

Global access and diversity

- Diversity: people and organisations shall accept and embrace diversity on the Internet as an asset for information sharing and innovation, even if it creates new challenges
- Trust in the Internet: trust is the essential component for further collaboration and growth of the Internet and will depend on how risk is managed, costs are allocated and effective remedies are provided;
- Universal availability and affordability: introduction of IPv6 to avoid lack of address space and possible fragmentation of the Internet in the near future

The trends and emerging values have something to say for the possible role and responses of government:

- Accept the loss of control and redefine the role of government as enabler of the context for self- organisation
- Assume a user-oriented approach in its governance role, being aware of the international dimension of anything happening on the Internet;
- Take a risk based approach to security, and consider supporting the uptake of risk reducing measures (like in "real life", such as pointing out risks of certain behaviour, or stimulate uptake of firewalls, etc, or even stimulate industry-wide investment in new protocols like IPv6)

- Aim to use new means to overcome old "divides" and at the same time be aware of possible new digital divides (locations, regions, generations, educations) that may need to be prevented
- Assess need for change in IPR policy whilst being mindful of its impacts on innovation
- Keep an eye open for new threats, for instance: how to deal with semantic attacks, and the role of public policy decision makers in addressing these
- Stimulate social innovation; collaboration between government and social networks; facilitating best practice
- Support and lead in the use of open standards and enabling interoperability
- Embrace communities of interest and collective approaches; decision making capability, accountability, representation and certification or endorsement of outcomes

In assessing these trends, values and the changing role of government the following picture emerges that could serve as a high level frame of reference.

Openness and transparency are essential character traits of the Internet economy and should be embraced by governments as necessary components to deal with issues of privacy, security and active inclusive participation. The creative and entrepreneurial individual – organised or not - is at the heart of this development and the open Internet is his habitat. In this world government does not only 'govern' but facilitates, enables, shares, empowers, creates awareness and stimulates trust. Government will also retain an important role in ensuring effective competition and supporting innovation, through the use of open standards and the application of intelligent but not overly restrictive IPR policies, which support the innovators and not the concentration of market power.

National and international government cannot effectively control or regulate this space and needs to embrace industry, service providers and other stakeholders in self-governing and co-regulatory arrangements. Governments may back these up and strengthen them through political, financial and sometimes regulatory means.

The virtual and the real world abide to many of the same rules, with human rights and respect for personal space as guiding principles. Also there are risks and benefits like in the real world, which need to be understood and managed. Yet at the same time it seems important to only take measures in areas where it is seen to be necessary, because of facts, rather then because of assumptions, in order to avoid that unnecessary barriers are created that would stop innovation in technology and its application in ways that may well be of benefit to society at large. The Internet economy is truly global and diverse, which creates many interesting opportunities for all, and connectivity and access for all should be supported wholeheartedly, notwithstanding some of the risks. To ensure this open, global character and free access, IPv6 has to be actively promoted.

CHAPTER 1 Introduction

The Internet is fascinating, and increasingly affecting our lives. The concept of a home-based global information system goes back at least as far as Isaac Asimov's short story "Anniversary" (Amazing Stories, March 1959), in which the characters look up information on a home computer called a "Multivac outlet" -- which was connected by a "planet-wide network of circuits" to a mile-long "super-computer" somewhere in the bowels of the Earth.[1] Yet it was less than 15 years ago that the World Wide Web (WWW) became public, released by CERN, where it was developed by Sir Tim Berners-Lee in 1989. The WWW and the Mosaic browser opened up the Internet to become what it is today.

The changes induced by the Internet and the pervasiveness of ICT offer endless opportunities and equally pose challenges for the individual and organisations as well as for society as a whole, which has a profound impact on public policy making. This study was conducted to support the Dutch Ministry of Economic Affairs input into the OECD ministerial conference at Seoul in 2008. The primary objective is to identify underlying issues and dilemmas that policy makers will face as the Internet economy [2] develops. It will analyse these in relation to the changing policy context in which the Ministry of Economic Affairs operates. The ultimate objective is to communicate the possible impacts of the evolving Internet economy on key areas and the resulting policy challenges to the Ministry of Economic Affairs, the government and the public at large, and to make suggestions as to how the Ministry of Economic Affairs may address them. The paper informs the reader of key issues and makes statements for discussion. This 'discussion paper' format was chosen to make the underlying issues more explicit and to trigger a broader debate on the effects (opportunities and challenges) of the emerging Internet economy. As this field is still very much in early development, an ongoing inclusive debate is needed rather than attempts to cast developments in stone. This does not exclude the possibility that at some point other measures may be needed to stimulate further take up and growth of the Internet.

[1] Wikipedia, http://en.wikipedia.org/wiki/Www#History retrieved on 21.12.2007

[2] The term used by the OECD to describe the increasingly central role of the Internet and ICT in our economies and the resulting changes in production processes, product development, productivity, supply chains, business models, global competition, etc.

The project started by selecting key topics and asking national and international experts to comment and rank them. The message to policy makers that broadly emerged from this expert consultation can be summarized as:

> *Keep the Internet available and open, by ensuring safe access and use - primarily by 'light touch' measures aimed at raising awareness rather than coercive intervention; and by embracing the Better Regulation principles of minimal, flexible and accountable regulation through appropriate self- and co-regulation, with special attention to issues of participation, transparency, compliance and control of spillovers (e.g. market distortions). Any residual adverse socio-political fallout should be dealt with through 'traditional' public policy measures.*

The consultation also delivered a clear ranking of topics. The topics that received the highest scores were summarised as:

- Security, reliability, privacy, and trust;
- Self regulation, international and multi-stakeholder Internet governance;
- Openness, accessibility for all of the network and net neutrality

Also deemed relevant but raising fewer concerns were:

- Social networking and new collaborative approaches
- Return on infrastructure investment; and the relationship between competition policy and innovation;
- Need and effects of global connectivity and access.

In two rounds of consultations it became apparent that several issues sparked disagreement among the experts (indicated by a strong variance in scoring) with regard to their relevance, or priority, for policymaking. As such we believe that these provide an indication of possible underlying dilemmas. These issues included:

- *Level of (actual or attempted) control by government*: can and should government control activity on the Internet as traditional jurisdictions and legal provisions seem increasingly inadequate?
- *Relation of private and public sector responsibility*: are these relations shifting and is government becoming just one of many players in the public sphere?
- *Relation and divisions between the real and virtual worlds:* how to deal with both, as one flows into the other? When do the virtual worlds have real world effects that would trigger a policy response, by whom?
- *Privacy: its relevance, universality and changing nature*: is the notion of privacy and the use of personal data changing, as comfort with and trust in the Internet as well as the possibilities to mine, store, manipulate and abuse such information increase?.
- *Role of monopolies; public subsidy and competition policy:* existing competition policy is challenged by tipping point tendencies, the emergence of natural monopolies and new collaborate approaches which improve speed and efficiency of research and technology development (RTD), innovation, product design.

- *Security versus uncertainty:* the Internet cannot be fully secured but online actors can secure themselves and their customers.
- *Trust: avoiding, managing and/or accepting risks:* full security online is an illusion just as in the offline world, thus anyone interacting on the Internet must manage risk and possible damage, whilst also accepting the 'public good' character of trust.
- *Identity versus anonymity:* identity is rapidly becoming the single organising construct for service delivery online, but people have various identities and may want to be in control of their use, and even be anonymous at times
- *Clashing values on an increasingly global Internet:* the Internet as a 'Western' invention and space ruled by 'Western' values and ethics of openness, transparency, privacy, fairness and security is changing to a global environment where all values can mingle and clash freely. Will 'Western' dominance have to give way or accommodate other influences?

These priority areas and potentially contentious topics were used as input to the expert discussions and further deliberations with the Ministry of Economic Affairs. The results of these discussions form the basis of this paper.

The paper first discusses trends and cross cutting issues, as well as emerging values and possible policy responses. In the Appendices it addresses the challenges and issues classified by the four main categories as defined by the upcoming OECD Agenda. These are summarised as: infrastructure; socio-economic developments; security and reliability; and the global nature and governance of the Internet. Under these four headings the paper focuses on the issues that were selected by the consultations and discussed in more depth in a series of expert workshops. The paper does not seek to be comprehensive by addressing all relevant issues that could be discussed at the OECD conference, but covers most of the scope.

CHAPTER 2

Emerging trends: Intensity of globally changing interactions and trade offs

The following general trends and underlying issues, which emerged from the expert seminars, are likely to provide the backdrop of future policy-making related to the emerging Internet economy. Every trend is followed by statements to inform and entice discussion.

2.1 Globalisation trends: Universal connectivity and access, and the cost and benefits of diversity

The global Internet population is growing and constantly changing: i.e. more people are connecting, from different geographies, with strongly diverging levels of knowledge, skills, speed, literacy and concerns over security. This continuous change is clearly reflected in statistics about world Internet usage[3].

Table 2.1 World Internet Usage and Population Statistics

World Regions	Population (2007 Est.)	Population % of World	Internet Usage, Latest Data (nr. of users)	% Population (Penetration)	Usage % of World	Usage Growth 2000-2007
Africa	941,249,130	14.2 %	44,234,240	4.7 %	3.5 %	879.8 %
Asia	3,733,783,474	56.5 %	461,703,143	12.4 %	36.6 %	303.9 %
Europe	801,821,187	12.1 %	343,787,434	42.9 %	27.2%	227.1 %
Middle East	192,755,045	2.7 %	33,510,500	17.4 %	2.7 %	920.2 %
North America	334,659,631	5.1 %	237,168,545	70.9 %	18.8%	119.4 %
Latin America/Caribbean	569,133,474	8.6 %	122,384,914	21.5 %	9.7 %	577.3 %
Oceania / Australia	33,568,225	0.5 %	19,243,921	57.3 %	1.5 %	152.6 %
WORLD TOTAL	6,606,970,166	100.0 %	1,262,032,697	19.1 %	100.0 %	249.6 %

SOURCE : www.Internetworldstatistics.com/stats.htm

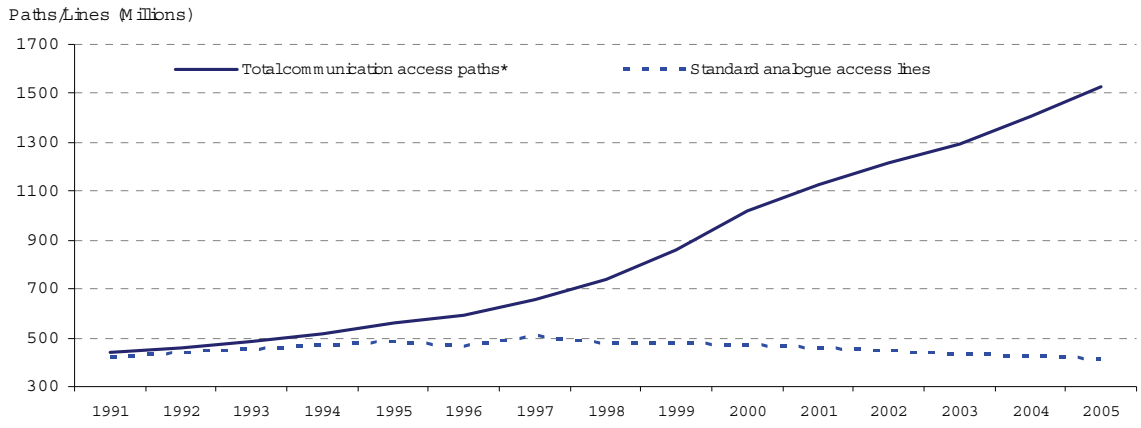
The statistics also make clear that the large majority of the world population does not yet have access, or is not actively using the Internet. Thus there is still a significant untapped

[3] Internet World Stats (2008) "Internet Usage Statistics", http://www.Internetworldstats.com/stats.htm

socio-economic potential of billions of consumers, entrepreneurs, innovators, creators, communicators, activists but also disruptors and criminals. The process of bringing the vast majority of the world population online will thus have significant impacts on both the online and real worlds. This will magnify the benefits that the Internet has to offer, as well as the associated threats and risks. Note however, that many of these promises and threats do not originate with the Internet, but rather are magnified or transformed by the speed, 'weightlessness', and global reach of online interactions.

A lot of research has shown the economic enabling power that the mobile phone has had in the developing world. Correlation between poverty reduction and the take up of mobile telephony is undisputed. Connectivity and Internet access is believed to generate similar positive effects, creating bigger markets, providing access to more information and new customers. The combination of the proliferation of mobile devices and new forms of mobile access could allow large groups in remote areas to leapfrog the barrier of absent fixed infrastructures; which holds significant potential for socio-economic development.

Different phenomena have different impacts across the world; For example, spam or viruses will be most harmful for those with slow equipment and poor security software and/or the greatest reliance on electronic mail. But there are strong negative externalities; unethical practices and/or insecure activities of part of the user community will affect the entire Internet. The relative cost of disruption is much higher in rich countries, where the Internet has become a highly critical infrastructure on which substantial parts of the economy depend. For less developed countries the economic impact of security failures can be expected to be lower and Internet policy priorities may emphasise other aspects, like take-up, training and access. Spill-over effects of security failures in other parts of the world can be substantial, caused in part by poor legal frameworks for computer misuse.



SOURCE: OECD Key ICT Indicators [www.oecd.org/sti/ICTindicators], 2007

Figure 2.1: Internet Access

Note: Total communication access paths = Standard analogue access lines + ISDN lines + DSL + cable modem + mobile subscribers.

Growth of the Internet benefits national economies by enabling globally collaborative innovation, increasing economies of scale and scope, opening up of new markets and

facilitating development. New businesses, supply and value chains are emerging through the global span of the Internet. However, its growth and global reach also raises concerns about security and risk of fragmentation of the Internet as new groups of users create their own environment (for example China or Arabic nations) or alternative environments which permit them to become less dependent on the governance decisions of the Internet Corporation for Assigned Names and Numbers (ICANN). Fragmentation of the Internet, where different groups are active in different spheres of the Internet and cannot easily communicate across these spheres, could pose problems to policy makers as the overall understanding is lost – conversely, the same developments *could* reinforce efficient and empowering decentralisation, specialisation and diversity.

Last but not least the growth of the Internet also impacts the availability of Internet Protocol version 4 (IPv4) addresses. The existing IP address space that allows users to connect to the Internet through different means, technologies and infrastructures is expected to run out between 2010 and 2011. This is expected to lead to a secondary market in IPv4 addresses, which will create entry barriers to those people who cannot afford the investment; which is likely to affect the start-up innovators and developing world more than the rest. To accommodate this shortage IPv6 has been developed, which is similar to IPv4 but has a nearly infinite number of addresses and contains extra security, mobility and auto-configuration features. Nevertheless take up of IPv6 by Internet Service Providers (ISPs) and connectivity providers has been disappointing and as such has not yet complemented IPv4; with all the potential risks of a new rich-poor divide on the Internet.

Statements for discussion:

- Connecting the unconnected creates substantial socio-economic opportunities, and Internet access should be seen as a human right
- Everyone has the right to participate freely in the cultural life of the community, to enjoy the arts and to share in scientific advancement and its benefits
- The openness of the Internet is its strength – driving innovation and inclusiveness. At the same time, rapid changes in the Internet population are challenging its governance structure and its self-regulating nature. This could lead to fragmentation (i.e. limit its beneficial openness).
- A global Internet is also a platform for diversity and will expose the current Western orientation to other values and influences. The 'West' will have to accept a reduction in its cultural dominance as global economic power shifts to new markets: 'our' truth will no longer be *the* (only) truth – this may benefit the world at large (one size does not fit all) and Western cultural values in particular.
- Introduction of IPv6 within the next 2 years is a necessity to avoid hindrances for new entrants

2.2 People trends: Being led by our kids and the empowerment of the individual

The changing composition of the Internet user population is in particular, driving the emergence of interaction-intensive uses like social networking and User Created Content (UCC). Their uptake is dominated by those under 24 in particular, who have grown up with the Internet.[4] These generations are shifting from being consumers of 'cool[5]' (passive) media like television to 'hot' (active) games and interactive content production & exchange.

This Web 2.0 world empowers individuals and groups to create, influence,[6] produce, transact, collaborate, and communicate globally, making them masters of their own empires – and therefore hard to steer or control by traditional mechanisms within existing institutions and jurisdictions.[7] Not for nothing did TIME Magazine nominate the Internet User 'you' (as in YouTube) as the personality of the year 2006[8]. This power 'at the bottom' steers activity towards places where self-organisation and expression, as well as collaborative participation, are facilitated. This can destabilise and disrupt established public or private institutions and business and/or governance models based on one-sided and one-dimensional views of interaction with individual customers, citizens,[9] voters,[10] patients, employees,[11] etc.

---

[4] OECD (2007) Participative Web and User-created Content: WEB 2.0, WIKIS And Social Networking, Paris: OECD; also Beck & Beck-Gernsheim (2001) Individualization: Institutionalized Individualism and its Social and Political Consequences London: SAGE Publications; Bauman (1997) Postmodernity and its Discontents Cambridge: Polity Press

[5] This characterisation of media dates back to MacLuhan and Fiore (1967) "The Medium is the Message" Bantam Books / Random House.

[6] Coleman (2005) "Blogs and the New Politics of Listening" The Political Quarterly, Vol. 76:2, pp.272–280; Cave (2004) "The Cure for the Ills of (e)Democracy is More (e)Democracy: Networked Governance in the Information Society", in: Cunningham & Cunningham (Eds) (2004) eAdoption and the Knowledge Economy: Issues, Applications, Case Studies, Amsterdam: IOS Press

[7] Coleman (2005) *Op cit.*

[8] Time Magazine (2006) "Time's Person of the Year: You" http://www.time.com/time/magazine/article/0,9171,1569514,00.html

[9] OECD (2001) Citizens as Partners, http://213.253.134.43/oecd/pdfs/browseit/4201131E.PDF

[10] Norris (2003) "Will New Technology Boost Turnout? Evaluating Experiments in E-Voting v. All-Postal Voting Facilities in UK Local Elections" John F. Kennedy School of Government, Harvard University, Faculty Research Working Papers Series; Lupia & Matsusaka (2004) "Direct Democracy: New Approaches to Old Questions" *Annual Review of Political Science* Vol. 7 pp.463-482; Kampen & Snijkers (2003) "E-Democracy: A Critical Evaluation of the Ultimate E-Dream" *Social Science Computer Review* Vol. 21 pp.491; OECD (2001) Citizens as Partners, http://213.253.134.43/oecd/pdfs/browseit/4201131E.PDF; World Bank Institute (2007) Beyond Public Scrutiny: Stocktaking of Social Accountability in OECD Countries, http://www.oecd.org/dataoecd/43/3/38983242.pdf

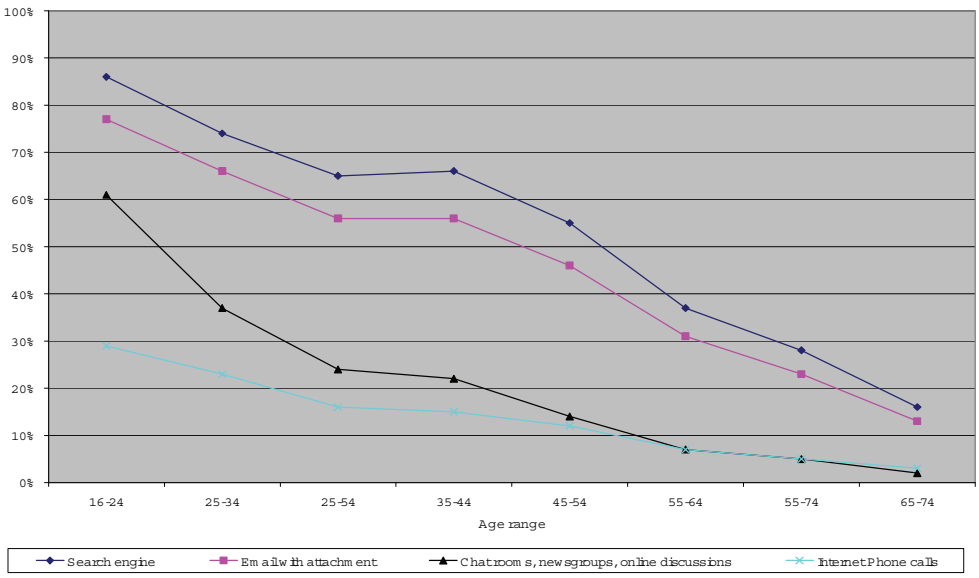
[11] Sennett (2006) The Culture of the New Capitalism New Haven: Yale University Press; Malone (2004) The Future of Work: How the New Order of Business Will Shape Your Organization, Your Management Style, and Your Life Boston: Harvard Business School Press; from RAND, "Living tomorrow: Germany in 2015"

These trends are particularly visible among the younger generation for whom the Internet and associated technologies and applications are intuitive. Not all participate in these new environments with the same vigour. Some individuals and groups do not participate at all, while others are immersed to a problematic degree. The digital divide remains, with large sections of the global population unconnected or connected only through analogue lines, and often without the skills necessary to navigate the Internet and benefit from available services and other opportunities (some of which never existed or no longer exist outside the virtual world).

As early as 1995 the digital divide was recognised as a socio-economic phenomenon.[12] Internet access and skills were and have remained heavily correlated with the socio-economic background and demographic characteristics of (potential) users. What is not known is the final pattern and extent of engagement and how many and who will deliberately choose not to exercise their entitlement to participate online. Their needs must be recognised and addressed as well, particularly by those (including, but not limited to governments) bearing public service responsibilities.

Figure 2.2 illustrates the correlation between age and the use of a number of new communication technologies. It also demonstrates that penetration differs across applications, as certain functionalities are easily embraced by older generations for which less of a digital divide is apparent. The gap seems to deepen with applications and functionalities that are more interactive and more multi-media and – as a consequence- less resembling of 'traditional' functions like mail and broadcast media.

Figure 2.2. Use of Internet applications by age group expressed in % of total group



SOURCE : Eurostat 2007

[12] For instance: Prof. Dr. Luc Soete, International economy, Chairman High Level Expert Group of the European Commission in the report "Building the European Information Society for us all"

Different global skill levels, connectivity and access determine the gap between the leading countries and the rest. New technologies[13] combined with unprecedented potential knowledge and market access that the Internet provides could allow people in developing nations to leap-frog historical development stages, with all the consequences of their large fixed capital infrastructures – especially in areas that do not yet have traditional Public Switched Telephone Networks (PSTN). Failure to grasp this potential continues to contribute to a widening divide between development 'haves' and 'have-nots.' Existing telecom infrastructures and antiquated regulatory arrangements in many developing countries strongly inhibit incentives for telecom operators to invest in new technologies and infrastructure, thereby attracting new service providers fit for local markets. Education and training is another barrier that needs to be addressed in order to increase the total skill base and the capacity of developing countries to generate, absorb and benefit from new possibilities.

These divisions between nations are reinforced by analogous 'divides' within them in terms of *access* (the ability to reach the Internet); *connectivity* (the ability to use the Internet to interact constructively with others); and *skills* (the ability to make productive use of the resulting opportunities). The combination of these factors in turn enables the 'take-off' of endogenous growth where growing outputs of knowledge- and interaction-intensive goods and services drive increased levels of knowledge and interaction.

Statements for discussion:

- Engagement with new Internet tools differs strongly between socio-economic groups and between regions; governments need to keep up and at the same time service all these groups even if such groups choose to remain deliberately unconnected.
- Creative and entrepreneurial individuals – alone or in organisation - are driving the change; Governments should foster this creative power and create spaces for self-organisation and not seek to perpetuate potentially obsolete concepts of control, without careful re-evaluation.
- This is not the first time in history that the young generation has more expertise and capability than their parents, but the extent and pace of the resultant changes are unprecedented.
- The way people think is changing; the minds of young people are developing to deal with many more simultaneous inputs significantly more information – often in the form of a diversity of isolated bits of fact and opinion. This contrasts with the simpler, less-informed, more reflective and slower pace of critical thought in prior times, with important consequences both for individual opinion formation, decision-making and society's response to new (and old) challenges.

[13] e.g. wireless, smaller and cheaper digital switches and rising cost-performance ratios.

2.3 Technology trends: a new era of pervasive computing creating intelligent environments

The Internet has already become a central feature in the everyday life of many (albeit no more than 20% of the world population today), but pervasive computing and ubiquitous connectivity are still assumed to be in initial phase of deployment. The real impact of these technological developments on society and the economy are only just emerging. There is wide recognition and implicit acceptance of technological imperfections, prompting users and system designers to factor this in when using the technology. Increased reliability will also increase expectations of quality of service and in turn make us more technology dependent.

Once these technologies interact seamlessly and people become comfortable with their use the real and virtual worlds will become more strongly coupled or more converged.[14] At first virtual worlds are expected to be environments for essentially non-spatial activities: gaming (Massive Multiplayer Online Games); social role play (Multi User Virtual Environments); and possibly for collaborative development and testing of products and social mechanisms. Later, with the benefit of geospatial services in which virtual and real worlds are overlaid or 'mashed' together, we can expect a more extensive rebalancing in which the allocation of activity to real and virtual channels reflects their true possibilities rather than historical precedent.

In addition to the merging of virtual and real worlds the trend towards more massive uptake of Radio Frequency Identification (RFID) is expected to lead to the 'Internet of things', where objects communicate among themselves. Typical examples might be tags on perishable products indicating to the refrigerator they are passed consumption date and the refrigerator automatically ordering from the online store. In addition, information on shops, products and institutions can be shared with people in the same geographical space; thus changing dumb objects into carriers of information.[15]

The embedding of intelligence in all kind of environments, processes and objects creates strong stimuli and removes barriers (both formal and psychological) to vastly increased creation and collection of data on the physical location and state of objects virtually all the time and everywhere. Potentially the lives of every human being (or selected groups) could be mapped in computer systems down to a very fine level of detail. The societal consequences of such developments can only be estimated, and how to deal with these kinds of developments requires conscious policy making that takes uncertainty (as well as the risk of clearly-foreseen possibilities) into account. The challenge for policy makers will partly consist of clearly identifying the risks associated with the deployment of these technologies and allocating the responsibilities for possible unforeseen consequences.

Whereas there is some concern among policy makers for fragmentation on the Internet, at the same time parts of the Internet are integrating into one big computer. This is called grid computing (also labelled 'Grids' or 'the cloud') including as much as timesharing of

[14] Metaverse Roadmap (2007) "Introduction: Roadmap Definition", http://www.metaverseroadmap.org/

[15] Note: in order to facilitate the need for abundant IP addresses here, introduction of IPv6 would be important

Central Processing Unit (CPU) capacity. Furthermore, the power of search engines and intelligent devices has improved the ability to easily locate (potentially) relevant information on the Internet, while at the same time the amount of information available via the Internet has grown exponentially. Some believe that new protocols and search techniques will evolve into the Semantic Web. This is an evolving extension of the WWW in which web content can be expressed not only in natural language, but also in a format that can be read and used by software agents, thus permitting them to find, share and integrate information more easily and in an autonomous fashion.[16]

Statements for discussion

- We are at the dawn of a number of technologies that will allow the creation of ambient intelligent environments, where things communicate continuously with other things
- Information on the environment (thus also related to individuals) will grow literally "by the minute" leading to issues of storage and data protection.
- The Internet will act like one big computer, all around us in the real world and as in the virtual space - these two environments are likely to merge or flow seamlessly together

2.4 Relevant security trends: Accepting risks, increasing transparency and taking precautions as in the physical world

It is impossible to predict what the uptake of Internet based services would be if security and corresponding trust levels were higher. Current intensive use suggests a high acceptance of the security risks and established trade offs between convenience, benefit, reliability and security. However it may be that the risks are not known, and also trust may in some ways be inversely correlated with security. The example of CCTV cameras in the UK shows that more security can actually lead to lower trust in government and higher concerns of insecurity.

With the increasing number of Internet users and the great variety of skills and risk levels, not to mention devices and range of software quality, the overall level of security of the Internet is expected to decrease. The nature of the Internet as a network of networks means that it is globally vulnerable to attacks from anywhere. At the same time we rely even more on the Internet for critical services, making security and reliability even more relevant.

The redundancy and openness of the Internet are still considered the best guarantee for its availability. Typically, threats to functionality e.g. whether messages can get through, etc. are mitigated by the redundancy and 'best-effort' character of the underlying protocols. In other cases security may be a combination of various safeguards, each of which is based on

[16] " I have a dream for the Web [in which computers] become capable of analyzing all the data on the Web – the content, links, and transactions between people and computers. A 'Semantic Web', which should make this possible, has yet to emerge, but when it does, the day-to-day mechanisms of trade, bureaucracy and our daily lives will be handled by machines talking to machines. The 'intelligent agents' people have touted for ages will finally materialize. " —Tim Berners-Lee, 1999

redundant protection (thus benefiting from the maximum performance among the different mechanisms), but which must all be in place (thus the overall level of system security depends on the weakest of the security components).[17]

Both security and precautions have some public good aspects (particularly the feeling of security that allows people to trust each other and results in rapid detection of threats and dissemination of counter-measures) and some private good aspects (e.g. the security of individual systems, which prompts defensive counter-measures that can damage inter-operability or shift risk to 'softer targets' who are less able to bear or manage the risks). The essential policy points are that openness may be the first casualty of individual (decentralised) attempts to shift or manage risk, and that the kinds of risk affecting open-by-design systems differ from those directed at (even attracted by) closed systems such as 'walled gardens'.

Securing the network itself would be detrimental to the Internet's openness and redundancy, believed to be its strongest assets. Many plead that security should be supplied at the edges e.g. appliances and users. Real security cannot be guaranteed over public networks. If this is required, in the case of military or law enforcement data exchange and communications for example, then it is supported by private networks, but all other traffic could be secured through effective encryption.

For specific applications secure sections or 'walled gardens' are expected to be established. Overall security, however, is a matter of allocation, management and acceptance of risk and corresponding costs and liabilities. The economics of risk and thus insurance will become more important than security technology. This requires transparency in what the actual risks are and how effective we can be in securing ourselves against these risks. This means that overall awareness of suppliers of services, ISPs and users should be improved and behaviour needs to change to create a stronger environment of trust and security.

As services change so do the security risks. The 'Semantic web' may be a bit further away, yet would again potentially revolutionise access to abundant online data available. Policy makers may want to support further development of this, even if this will compromise the ability to protect ones personal data.

The coming third wave of information attacks - semantic attacks – is likely to target data and its meaning. It may include fake press releases, false rumours, and manipulated databases. The most severe semantic attacks would be those against automatic systems, such as intelligent agents, remote-control devices, etc., that rigidly accept input and have limited ability to evaluate. Semantic attacks are much harder to defend against because they target meaning rather than software flaws. They play on security flaws in people, not in systems.[18]

---

[17] H. Varian (2004) " System Reliability and Free Riding" Advances in Information Security vol. 12:1-15 and Geoffrey Heal and Howard Kunreuther (2002) " You Only Die Once: Managing Discrete Interdependent Risks" at: http://www2.gsb.columbia.edu/faculty/gheal/EconomicTheoryPapers/discrete.pdf.

[18] See also Bruce Schneier, Crypto-Gram Newsletter, October 15, 2000 and October 19th 2007, Web 2.0 Conference in San Francisco

Statements for discussion

- The economics of risk and insurance will become more important than security technology.
- Security should be applied where it is most appropriate. The Internet can be compared to a street or other public space; it has some ground rules but essentially you enter at your own risk; whereas private networks and 'walled gardens' - like houses, banks and other private spaces - offer security and a safer environment. In the latter case, you trust the environment, in the former you trust the people in it.
- The risks of 'being on the street' could be reduced by 'streetlights in cyberspace' (making risks more explicit and visible) and/or cyber policing; even if such actions have limited effectiveness they can signal an active and collective will to tackle cyber crime.
- Full security is unachievable, costly and undesirable - it would reduce the openness of the Internet and freedoms of assembly and communication; instead users from public, business and civil spheres should actively assess and manage their risks in an environment that informs and empowers them to do so.
- Security is achieved or undermined by allocating accountability, responsibility and liability for damage, and thus depends on who participates and what incentives they face. Cost, benefit and risk profiles differ across stakeholders; the resulting differences in willingness to pay for insurance and management of risk and damage can be exploited for good or ill.

2.5 Relevant economic trends: Balancing collaboration and competition, stability and innovation

The Internet already has had a profound impact on the global economy. Its effects are slowly permeating into all aspects of the economy and the way business is conducted. Emerging business models increasingly build on sharing of information and opening up of (formerly) critical and highly protected processes, including Research and Technological Development (RTD) and innovation. This reflects the increasing recognition of the inherent nonlinearity of innovation and diffusion and the falling transaction cost of collaboration. Nonlinearity has three specific manifestations:

1. the critical importance of feedback loops up and down value chains (e.g. innovation by customers or end users);
2. the existence of multiple channels through which innovations produce economic benefits (e.g. exploitation of intellectual property, facilitation of organisational innovation, improvements in the productivity consequences of infrastructures and public services);
3. the existence of 'critical mass' thresholds in time, character, and space. Time is affected by take-off adoption pathways, whereas characteristics are determined by innovation clusters that evolve around key technologies or uses; and space is defined by the emergence of regional clusters capable of competing on a national, European or global scale against large multinational enterprises.

At the same time, improvements in ICTs make communication, joint working and collaborative innovation faster, cheaper, more secure and richer. The combination of these factors with increased labour mobility and the rapid pace of technological change mean that economic activity is increasingly organised in terms of networks of interacting units. In some cases, this takes the form of flexible and evolving (often short-term and purpose-built) partnerships and alliances, but – at least in some market sectors – firms themselves are evolving into networks of experts collaborating in loose project teams.

Product development through mass collaboration (including the open source movement) is proving to be productive far beyond such well-known examples as Wikipedia and Linux. Together with new forms of open innovation, collaborative approaches to invention, product design, development and marketing are producing (by comparison with traditional methods) much faster and cheaper results. More importantly, the resulting goods and services are both closer to consumers' needs and the basis for more sustained engagement with consumers, as they are drawn into the product and services development process. Often such contributions are free and based on recognition, more than monetary reward. This engagement is of critical importance in a highly mobile, rapidly changing and globalised economy, since it forms at once the basis for a sustainable market position and the vehicle through which the fruits of innovation can be embedded in local (e.g. national or regional) economies, or can be transferred from one sector or domain to another. Without the prospect of such sustainability, embedding, or transference, the incentives for long-term investments and the course of future development will be weakened or distorted.

There are also changes in the roles and participation of smaller enterprises, which can redress at least the adverse consequences of recent trends towards concentration and the dominance of large (often multinational) corporate entities. SMEs and individuals now have access to the computing power, the connectivity and services that used to be reserved for large organisations. Their flexibility and agility will challenge large incumbent enterprises, which are tied up in legacy systems and are more likely to defend obsolete business models.

These developments are already changing existing supply chains, the productivity impacts and strategic uses of intellectual property rights, and relationships among rival and complementary firms, between employers and employees, between customers and producers and between firms and regulators. They will affect the governance and accountability arrangements of enterprise; as well as the core function of commercial organisations changing from producers to brokers, financiers, quality certifiers and network managers. Even the basis of competition is changing: from sales to access, from direct transactions with customers to two (or more)- sided 'platform competition' and from competition in terms of the price, quality and features of the currently-offered goods and services to the 'real option' represented by future, innovative goods, services and interactions opened up by subscribing to a particular service bundle. In general, future products are increasingly likely to be viewed, developed, marketed and purchased as services, particularly as the components of the 'wireless network of things' start connecting and communicating and as the costs and benefits delivered by such connected devices becomes less dependent on their own embedded ICT.

New collaborative approaches and bottom up innovation also affect the effectiveness of intellectual property rights (IPR). Traditional IPR monopoly power may not be optimal in the specific circumstances of the Internet. Three examples illustrate the point. The first involves interoperability – if the value of a good or service increases as more people use it, it may be profit-maximising to retain strong IPR protections, but to enforce them only on high-value, low-elasticity users – the 'violations' by low-value users sacrifice relatively little revenue but expand the user base and thus the willingness to pay of high-value (e.g. corporate) users who *will* abide by IPR rules. The second concerns the production of complementary innovations – a profit maximising inventor will wish to make access to his innovation freely available to producers of complementary goods in order to reinforce a critical mass and a *de facto* standard. To some degree, this leads to tipping and the risk of excessive volatility (as innovators rush to the new potential market leader) or excess inertia (as firms avoid the risk of stranded investments in an obsolete technology), but the benefits of complementarity and the possibility to negotiate or trade around these risks provide strong arguments for more flexible arrangements – again, with a range of negotiable duration, bundling and strength to avoid the consequences of a one-size-fits-all system. Finally, the importance of user-generated innovation and other sources of inventive activity not motivated by monetised profits suggests that the use of markets to motivate and control innovation has its limits, and thus that Creative Commons, the General Public Licence (GPL), compulsory licensing and 'social IPR' all have roles to play.

Statements for discussion:

- The new paradigms of open innovation and collaboration and of dynamic innovation networks better capitalise the collective knowledge of industry and independent researchers/entrepreneurs; however such collaboration may facilitate anticompetitive behaviour (entry deterrence, predation and collusion) towards new entrants and others in the value chain, through strategic use of standards, price and market-sharing agreements, etc.
- The tipping point tendencies (in terms of steep adoption curves and winner-takes-all equilibriums) of the information economy imply that fast adopters (and adapters), rather than innovators may be best placed to capture the lion's share of benefits from innovation, even when the original innovations arise in other sectors or countries.
- The Internet economy threatens many incumbent organisations with disruption, evoking defensive reactions to shore up existing business models and subvert the new, fast-moving paradigm.
- Governments (especially acting together to track the changing need for regulation and the potency of alternatives to regulation) can help to smooth the transition and manage the resulting volatility, but must accept that change has its casualties and investment should not be wasted on defending obsolete lines of business.
- At the same time, policy makers must recognise that not all novelties represent advances, and that complementarity may be as important as (global) competition. Thus, if all countries invest in the same "strategic" technologies, the development of comparative advantage may be suppressed.
- Much of the value created by investing in new infrastructure is not returned to the

investor, but accrues to service providers and consumers. This could be a disincentive to invest, though this phenomenon is not broadly observed, as returns are possibly still sufficient. In case underinvestment occurs, different forms of gain sharing or investment incentives may become necessary.
- IPR is loosing effectiveness as a tool to foster invention and innovation and is regularly applied defensively to avoid disruptive innovation to take place (e.g. in the music industry).

2.6 Governance trends: accepting the global, multi facetted nature of the Internet and dealing with failing jurisdictions and poor enforcement

National governments are loosing control over the behaviour of 'their' citizens as the definition of national jurisdictions and the rules of international private and penal law are not adjusted to the borderless Internet world. Enforcement of existing rules and of new measures based on traditional regulatory instruments is proving challenging if not impossible. When assessing the legal competence over virtual worlds another dimension of complexity is added.

It is safe to say that traditional regulatory and governance instruments fail in the Internet world, but that there are no proven alternatives yet. Nonetheless, the Internet has given rise to a wide variety of self- and co-regulatory schemes,[19] which offer potential advantages of speed, adaptability, efficiency and effectiveness to the extent that they are based on the active participation of informed stakeholders with direct powers of action. Compared with formal regulation, such arrangements can lead to greater commitment and *buy-in* by stakeholders, higher levels of *compliance*, *reduced cost* (both for the state and in general), *flexibility* in response to changing circumstances and challenges, greater opportunities to coordinate governance of inter-related issues and engage those best able to inform policy, ensure compliance, etc. Behind many of these advantages lies one that is valued in its own right; the engagement of specific forms of *expertise and knowledge* in the regulatory process. Finally, self- or co-regulation can enhance the *impact and sustainability* of sector governance.

As approaches for self-regulation in industry are slowly evolving, they also raise some concerns. Forcing stakeholders to self-regulate may lead to cartel behaviour through closing out newcomers. In practice, many of these initiatives depend on personalities, their knowledge, drive and networks, without solid institutional embedding, thus suffering significant continuity risks. Moreover there is a large diversity in these approaches, with differing effectiveness and maturity, enforcement capabilities, and institutional bases. Also, it is inherently difficult to define the relevant stakeholder group, to enforce measures, to institute a working arbitration mechanism, and to involve newcomers. Sometimes these schemes give the impression that concerns are addressed, but in fact (deliberately or not)

[19] Essentially, self-regulation involves collective governance by non-government stakeholders, while co-regulatory schemes involve government participation in the form of delegated powers, state means of enforcement of rules and/or a 'backstop' regulatory power in the event of governance failure.

are acting as mere 'Potemkin villages'[20]. This all raises legitimacy questions, especially as to the level of stakeholder involvement and acceptance. Decisions need to be transparent and have legitimacy beyond the members of the group. [21] Also, the quality of these schemes still differs widely between countries and regions has to be taken into account.

To be effective these schemes need to operate in a regulated space and be backed up by co-regulation or the threat of full regulation. Governments should therefore carefully monitor these to see if and where additional pressure should be applied. In general governments should acknowledge the benefit of the existing multi-stakeholder approaches and endorse and support them and strengthen their institutional base. Notwithstanding some of the weaknesses noted, these schemes are undoubtedly the way forward in organising and governing activity that cannot be controlled through traditional regulatory instruments.

Finally the Internet as a global infrastructure needs a global governance structure, which is discussed in a number of global initiatives.[22] This is a formidable challenge, because the context is rapidly changing and the approaches are all new and experimental. Principles of good governance that should guide the process include transparency, accountability, targeting, proportionality, consistency, wide participation and exchanges of good practice. The primary focus should be on removing unnecessary cross-border barriers (legal, value based, contradicting interests and other, standards and protocols) and strengthening existing processes, whilst being flexible to allow adjustments to ongoing change and uncertainty. In all of this it must be made clear what the value is to the users whose concerns are at the heart of the Internet – but situated at its edges.

Where necessary, national governments may want to take the lead in removing unnecessary barriers by championing multi-stakeholder governance at international Internet governance platforms and by leading by example. A general guideline would be to take the user as the measure.[23] This could range from "intuitive clarity" of Internet rules that are as much as possible consistent across countries, to removing specific barriers that prevent development of Internet activities as the benefits of such barriers remain unrecognised. Other ways in which Governments can set the example is by recognising the emergence of new 'commons' and releasing public sector information as part of it, but also making clear the value of governance and preparing for the unknown.

---

[20] Expression used in the workshops in reference to cardboard villages in Imperial Russia portraying a false image of wealth and development, hiding the true reality of rural poverty: i.e. creating a facade

[21] The advantages, together with potential disadvantages and risks and other aspects of the design and implementation of 'Better Regulation' in this area have been described in a recent report to the European Commission: Marsden, C. Cave, J. and Simmons, S. (2008) "Options for and Effectiveness of Internet Self- and Co-Regulation" Report for European Commission, DG INFSO.

[22] Dutton (2006) "Addressing the Issues of Internet Governance for Development: A Framework for Setting an Agenda for Effective Coordination" , Oxford Internet Institute, University of Oxford, http://www.intgovforum.org/Substantive_1st_IGF/Dutton-IG4D-30July06.pdf

[23] More detailed guidelines are given in Appendix A: Thematic Discussion to this paper in the section dealing with governance

Statements for discussion:

- Self-governance and full involvement of relevant stakeholders are essential building blocks for future Internet governance
- Industry self-regulation should be closely monitored for its ability to enforce its rules and inclusiveness of all relevant stakeholders; to be effective these schemes need to operate in a regulated space and be backed up by co-regulation or the threat of full regulation.
- Multi-stakeholder approaches risk having continuity problems and are challenged to define the range of stakeholders to include, but as some have already proven (ICANN, IETF) these schemes are an essential complements to traditional regulation and must be actively supported, professionalized and institutionalised
- International governance is necessary to deal with global issues and ensuring effective functioning of the Internet, following principles of good governance. However, it is in its infancy, understaffed and facing an up-hill struggle against vested interests. It should be considered whether folding back current initiatives into existing multilateral governance structures could be effective.

CHAPTER 3 Emerging values: Redefining how people and organisations interact

The trends and changes that are described in the previous chapter also affect the perceptions of the world around us. From the expert consultations and seminars a number of 'values' emerged that seem to underpin the discussions of the future Internet economy, though they are clearly not universal. Their appreciation differs between stakeholders, and between generations and cultures, between active Internet users and the sporadic. Given their fluidity we use the phrase 'value dimensions' as a term of reference.

3.1 To know and be known

In the dichotomy of openness versus security it can be stated that users want to be 'protected and not spied on'. The world of the Internet and particularly new virtual worlds like Second Life are the space of the people, where they decide to be anonymous and/or choose their identities. In this environment interference of government is widely rejected as overly intrusive and largely ineffective. On the other hand, the law enforcement and intelligence communities would like to access the exchange of data and communication and use modern profiling and search techniques in the fight against organised crime and international terrorism. A way forward is to create transparency in the way data is used and by whom and to ensure wider application of the right to consent. In addition, adequate measures should be in place to ensure that anonymity and thus privacy is only broken when sufficiently justified. In many ways this is comparable to the limitations for police forces to enter private homes, yet the key difference is that these limitations are currently very much bound to a clear local legal context, that differs between countries, yet the applicability of national law is only possible within the physical borders of a nation. In the Internet space, this is not evident.

Privacy is a topic of much discussion, with some claiming that it does not exist in an Internet age of full transparency and others stating that privacy protection is the most important condition to be fulfilled for the full exploitation of the Internet's potential. Furthermore, it is clear that the concept of privacy as such is very much dependent on cultural stance and personal preferences. Breach of privacy can occur when data on persons are collected and used without a justified basis. In this it is important to note that personal data is not necessarily owned by the data subject although he or she should be in a position to control it. People can decide to trade personal data – which is their economic right - and bear the consequences. Here education and awareness raising activities could be considered

adequate policy responses. The danger is not so much the use of the data itself, but the use in different contexts, as the implications that are drawn from the data are highly context dependent.

There is a strong wish to ensure that someone's privacy cannot be breached: it is commonly seen as a fundamental right. Therefore, use of data should only be allowed for the purpose it was collected for[24]. A tentative definition of privacy could be: "the right not to be spied on and the right to keep secrets, and possibly even the right to certain anonymity." We like to control how we present ourselves and to whom. We may be very open about certain aspects and decide to shield others; depending on our objectives, cultures, beliefs, present social environment etc. The fact that people want to be unique and even go as far as branding themselves as unique personalities on the Internet, does not imply – even if someone 'bares all' - that the control over privacy is forgone. Our identities consist of different elements and we want to retain control over them.

People also have multiple identities, which they use in different contexts. The Internet environment and the services – particularly eGovernment – should be aware and respectful of this. People may be employee, employer, patient, citizen, etc. all at once. When representing the company someone may not want to do this in a private capacity; also one does not vote as an employee in general elections, but as a citizen with equal rights.

3.2 Awareness and trust

Raising awareness of the way data is used has already mentioned. Awareness of overall risks on the Internet is a broader issue, which relates to the acceptance and management of the cost of risk. As full security will not be achievable for all under all circumstances, trust in the Internet will depend on ways how risk is managed and its costs allocated. Transparency of the nature of the threat and scope of the risk are critically important to make effective assessments of one's own risk profile and possible exposure to costs.

Trust is key to enable eCommerce and interpersonal transactions and communication. Justified trust (i.e. trust based on true security as delivered by the system) is an important means to keep down transaction costs. The new Internet environment is developing informal trust codes and etiquette; to self impose decent behaviour on a tit-for-tat basis. Relationships are allowed to develop and grow to build trust and familiarity step by step. However, the complexities of the virtual world make it very opaque and almost impossible to effectively assess personal risks. In this environment trust and mechanisms to establish and enforce trust are crucial. At the same time trust is very dependent on individual risk assessment and risk preferences. It is worth noting that, despite the lack of transparency, the number of Internet users continues to grow. And judging from the trends in online transactions, many perceive the risk of misuse to be acceptable. In addition to the acceptance of risk, new self-organising (user-led) assessment mechanisms like tagging, peering and ranking e.g. with sites like www.ciao.co.uk and www.pricerunner.co.uk support the development of trust.

---

[24] OECD Guidelines on the Protection of Privacy (http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html)

3.3 Accountability and the power of the collective

Sharing, transparency, and fairness - the new Internet world is a place where self-organizing is – or should be - enabled, where sharing ideas, and opening up processes, means receiving inputs – often for free. Businesses open up their product development to consumer feedback and mass collaboration, and have problems solved through open queries and competitions. The reward may be a prize, a share of profit, or just recognition. People are willing to contribute more than they receive back; thus contributing to creative commons. Governments may also find that opening up their processes, sharing public information, and actively engaging citizens to take an interest in the public (virtual and real) space leads to ownership and shared responsibilities.

An important value will be how responsibility is allocated and assumed, and how accountability is established in a time where processes become collective endeavours. Mass collaboration and voluntary agreements provide good approaches for innovative development processes, drawing on the knowledge and talent of many. However they lack effective decision making capabilities, quality control and the endorsement (certification) of the outcomes, thus potentially leading to instability and uncertainty about the quality and value of the process outputs. Peer review, ranking, karma points and the like, are expected to fulfil some of this function but are easy to manipulate and are not evidence based.

3.4 Accepting Diversity

Values dominating the Internet have been mostly Western. With global connectivity that is expected to change. For this, again see the Table 2.1 on World Internet Usage on page 19 which shows that the biggest growth countries are in Africa and Asia. The 'globality' of connectivity may be undermined, as some of these fast growers (such as China or Arabic countries) use different character sets than currently in use on in the Internet's Domain Name System.

The Internet is undivided and truly global. It should be accessible to all, to allow old and new users all the benefits that it brings. As access and connectivity have become such important conditions for participating in large parts of the global economy, in social interaction, cultural expression and democratic/civic participation; they should be considered as universal fundamental rights. To ensure that access and use is technically feasible for the mid and long term, IPv6 has to be adopted on a wide scale as soon as possible, before IPv4 addresses run out (see section 2.1).

Emerging value dimensions:

Identity and privacy

- Control over personal data: people do not own personal data, yet should be in a position to control it;
- Privacy: the use of private personal data must be sufficiently justified; people want to be protected and not spied on;
- Anonymity: people have the right to keep secrets, and possibly even the right to

certain anonymity;
- Multiple identities: people's identities consist of different elements and they want to retain control over them;

Transparency and openness
- Transparency: people require transparency to enable them to decide about the desirable level of privacy and their security risks;
- Responsibility: people and organisations need to define how responsibility is allocated and assumed, and how accountability is established;
- Sharing, openness, and fairness: people self-organise and private and public organisations will facilitate this as they are aware that a lot more can be achieved and many more people can be engaged by opening up processes and information and inviting active participation.

Global access and diversity
- Diversity: people and organisations shall accept and embrace diversity on the Internet as an asset for information sharing and innovation, even if it creates new challenges;
- Trust in the Internet: trust is the essential component for further collaboration and growth of the Internet and will depend on ways how risk is managed, costs are allocated and effective remedies are provided;
- Universal availability and affordability: introduction of IPv6 to avoid lack of address space and possible fragmentation of the Internet in the near future.

CHAPTER 4 The changing role of government; between idleness and engagement

The shifting landscape affects the role of key stakeholders, government in particular. In this chapter a few responses to the broad range of challenges facing government are discussed. These are mere pointers in a very complex and fast-moving environment of interrelated policy fields. More detailed suggestions, particularly on governance, co- and self-regulation and Intellectual Property Rights (IPR), innovation and competition policy can be found in Appendix A: Thematic discussion: delivering a strong message at the OECD Ministerial Conference.

4.1 Public goods for all

Governments' role is to ensure a certain level of *"security"* and *"public order"*, while accepting that - as in the real world – there is no such thing as 100% security. There will always be risks, which vary from user to user and which need to be assessed and managed appropriately. Such risks included breaches of privacy, impersonation, attacks on reputation, identity theft, semantic attacks, etc. The government should concern itself with making users (citizens, businesses and government itself) more aware of the risks and the responsibilities to deal with these, whereby government can ensure certain minimal security parameters and guarantees. It can also stimulate the development of tools for protecting the 'weak' – e.g. children against abusive content - in society. By increasing overall awareness, providing effective remedy against abuse, leading by example in applying effective data protection policies and working with industries to fight cyber crime, government can help ensuring overall levels of trust in the Internet remain sufficiently high.

Policy makers will be challenged to keep up with the growing group of (young) active Internet users that are driving the new Web 2.0 paradigm; and they will need to ensure that in the mean time the *digital divide* will not increase, i.e. ensure involvement of the 'digital laggards'. In doing so they will need to acknowledge that a substantial minority has taken the conscious decision to remain unconnected, while others simply do not see the benefit, fear technology, have concerns for security or privacy, or cannot afford the necessary devices or high speed connections. As a starting point the government should ensure that all those that can and are willing to be connected have access at reasonable price and adequate speed. There remains a need to improve skills to allow people that are willing but unable to be active on the Internet to participate. Finally government must

accommodate the offline world. Government is different from the private sector – the public sector does not choose its customers and must respect those that for some reason remain unconnected. It may want to take particular care that these groups are not excluded from public services and other important parts of socio-economic life.

Overall the growth of the Internet and the increase of the total population of people having access to the Internet is a good thing. It provides a wider reach, opens up bigger markets, enables development and the emergence of new businesses and value chains. It also unlocks information for people formerly deprived of information and creates chances for personal development and learning where this was previously impossible. At the same time this requires attention in ensuring adequate security, transparency and connectivity of the Internet. The OECD and other international frameworks should be used to address these *global disparities*.

4.2 Dealing with virtual worlds

Should virtual worlds be regulated by government, or do virtual communities display sufficient capabilities of self-regulation? Two kinds of virtual worlds can be distinguished: Massively Multiplayer Online Role Playing Games (MMORPG) e.g. World of Warcraft on one hand and Multi User Virtual Environments such as Second Life on the other. In games the role of the provider is more active than in the second category, which has implications for enforceability of rules.

Developments might be too quick for efficient regulation to emerge. However, the potential impact of these *alternative realities* seems sufficiently high to justify an active public role. At this time it may be too early for distinctive government intervention. Through assessments and monitoring of development, governments could remain involved in virtual worlds, without actively intervening, or retracting completely. This is important in order to understand the implications for current public service and regulatory obligations, but also to identify opportunities to expand services of general public interest or withdraw from provision of (direct and regulatory) services that may no longer be required or appropriate.

4.3 Governing the ungoverned

Governments should accept a new reality, in which they no longer attempt to find more effective ways of regulating economic activity, social behaviour (e.g. privacy, content, etc.) or technologies (spectrum access, standards compatibility, quality of service, etc.) but rather recognise that these objectives and the participants are extensively cross-linked in a complex system that ignores national or geographical boundaries. This system cannot be controlled because there is no body that stands outside the system and combines a balanced and informed view of what is possible and desirable with the power to compel good and acceptable outcomes. What is needed is a suitable 'sandbox' to allow experimentation with *new methods of governance* to proceed in parallel with effective operation of 'legacy systems' until better approaches can be identified and their risks managed.

Some apparent opportunities can already be embraced. In particular the opportunity for policy-makers and politicians to engage with citizens in much more individual and hands-on ways has aroused the interest of policy makers around the globe. Indeed, both the internecine (e.g. the interaction of different jurisdictions in these new shared spaces) and fundamental (e.g. the changing nature of democratic participation and accountability) prospects opened up by these developments, merit and demand new approaches. How to effectively leverage existing or deploy new communities of interests in policy development processes and ensuring legitimacy of outcomes to the general public is part of the challenge and the solution. Existing processes of representative democracy, which serve the legitimisation of process outcomes need to be aligned with these *new forms of public engagement*. Certification and official endorsement by public authorities of the work of such communities could help to re-enforce their legitimacy.

4.4 Between collaboration and competition, supporting innovation

Government's role in supporting economic activity and especially *innovation and competition* is also changing. There are continuing tensions between the dynamics of the Internet economy (in particular the strong potential for sectors to be controlled by one or a few dominant firms and for early leads in innovation to convert into sustained market dominance) and the potential efficiency gains offered by innovation. As with other high-technology areas, the balance depends in large measure on a combination of governance by market forces – particularly through markets for knowledge created by IPR systems – and regulation systems created to assist in correcting the causes or mitigating the consequences of market failure. It is worth noting that the speed and scope of knowledge diffusion on the Internet extend the potential force of competition (both of firms and of ideas) to global scale; at the same time, the same factors provide a global playing field on which market power can be exercised, and thus stronger incentives to invest in market control.

The Internet economy rests on a wide *range of property rights*; in addition to IPR, other intangible (e.g. spectrum) and tangible property rights play key roles in enabling and shaping market and non-market value-creation. The 'right size' (duration, scope, etc.) of IPR and other intangible rights in the Internet economy is not constant (the way patent law assumes) but changes with the pace and nature of technology, business models and societal development.

Much the same need to balance technological, economic and societal forces is found in public *alternatives to the 'private property paradigm' of IPR* (namely standardisation) and to other forms of regulation. The Internet's development is of concern to a range of regulators concerned with technologies (generally sector-specific regulators), economic effects (often competition authorities and trade ministries) and societal regulation (education, health, public safety, security, etc. ministries). The effects with which they are concerned are far more tightly interconnected in the Internet and in relation to affected stakeholders than the ministries themselves are – a key challenge is thus an appropriate balance between competition (with all its diversity and churn) and co-operation. This general principle applies to innovators and participants in the Internet. It applies no less to those charged with regulating and supporting its development.

Finally, it is worth recording that government, business and civil society share many interests in the outcomes - business competition is only one of many forces influencing Internet development. The alignment of interests, placement of risk and dangers of capture are all important in considering innovation initiatives relating to government support for *RTD and deployment*, business RTD and investment, civilian collaborative innovation, etc.

Statements for Discussion

Governments should:

- Assume a user-oriented approach in its governance role, being aware of the international dimension of anything happening on the Internet;
- Take a risk based approach to security, and consider supporting the uptake of risk reducing measures (like in "real life", such as pointing out risks of certain behaviour, or stimulate uptake of firewalls, etc, or even stimulate industry-wide investment in new protocols like IPv6)
- Aim to use new means to overcome old "divides" and at the same time be aware of possible new digital divides (locations, regions, generations, educations) that may need to be prevented
- Assess need for change in IPR policy, mindful of its impacts on innovation
- Accept the loss of control and redefine a role as enabler of the context for self-organisation
- Keep an open eye for new threats, for instance: how to deal with semantic attacks, and the role for public policy decision makers
- Stimulate social innovation; collaboration between government and social networks; facilitating best practice
- Support and lead in the use of open standards and enable interoperability
- Embrace communities of interest and collective approaches; decision making capability, accountability, representation and certification or endorsement of outcomes

CHAPTER 5 Concluding Remarks

This is an interesting time for policymaking; requiring patience, insight and the right tools to effectively benefit from the opportunities and address the challenges presented by the Internet economy.

It is too early to say if we are at the point of a paradigm shift, in which the role of government will be fundamentally different. However the underlying trends and emerging 'value dimensions' of the policy environment suggest that significant flexibility is required and that many of the traditional public sector tasks are changing, with new actors entering the game. Also, the instruments of government appear to have lost much of their effectiveness and new constructs are required.

This paper should help government in understanding and embracing evolving realities: of the Internet's global scope and the empowerment of individuals; of the acceptance of risks and importance of trust; of the power of the collective and the need for transparency; of people that want to hide and others that do not care, those who participate and those who log off. Some ideas for government are thus provided in this paper. The recommendations are mere pointers to make policy makers aware of the complexities and uncertainties and possible steps to address these.

APPENDICES

Appendix A: Thematic discussion: delivering a strong message at the OECD Ministerial Conference

This Appendix serves as a briefing document for the OECD 2008 Ministerial Conference on the future of the Internet. The outcomes of the literature review, relevant ongoing RAND Europe studies, expert consultations, and seminars were structured to mirror – where possible - the OECD Agenda. The agenda is an evolving document and the inputs for this paper were based on previous versions, therefore some differences in terminology may occur, though most of the topics are covered.

Theme 1, Infrastructure: Facilitate the convergence of networks and devices, applications and services

Defining the term 'Infrastructure'

Before discussing 'infrastructures' it is important to define what infrastructure means to distinguish between "hard" and "soft" infrastructures and to understand possible complexities. Hard infrastructures contain wires, switches, terminals etc, whereas soft infrastructures, which exist on top of or alongside hard infrastructures can include knowledge infrastructures e.g. search engines, the "semantic web" etc.

Questions arise such as: are critical services part of the infrastructure or do we only include the underlying layers of hardware and equipment? Although there is no overriding agreement on this, for policy purposes services should be separated from infrastructure, as the defining element is that in services there is a choice, and in infrastructure not. Even with services that have the characteristics of infrastructure – like Voice over Internet Protocol (VoIP) – there mostly are alternatives available and thus should be kept out of the discussion on infrastructure, even though this may be arbitrary at times. The approach depends on the issue and context that regulator wants to address; e.g. market power, public service provision, or dynamism of the sector, whereby the focus should be on the consumer, not the producer.

As the Internet is evolving into one global computer, the hardware at the ends – e.g. PC's – should also be considered as part of the infrastructure. As every infrastructural layer has different players, policies have to be layer specific; even if the same players are vertically crossing layers, they have different roles at different layers.

Convergence

A specific issue is convergence: platforms that were traditionally used for media, telecommunication or data communication are increasingly supporting all of these services. In a way this accelerates developments, as these infrastructures compete and one would expect that the most viable business model will survive (the business model that is best able to serve consumer interests, as in the end it is the users that will pay the bills). This process of convergence is thoroughly disruptive for incumbent telecommunication providers with large capital investments in fixed infrastructures, for which they are used to receiving rents. The services over these platforms and infrastructures are converging, leading to a radical challenge to the business models of traditional service providers like broadcasting organisations and telephony operators, which often respond by displaying anti-competitive behaviour in defence of their habitual revenue streams.

IPv6

An important issue in ensuring sufficient capacity on the Internet to deal with growth of access and new forms of use – like objects with IP addresses - is the transition from IPv4 to IPv6. IPv4 is still providing most of the functionality people expect for free, and IPv6 is not perceived to add much. There are no IPv6 based services yet that would justify the transition. Thus there is currently no incentive for a move to IPv6, which in itself does not have to be a problem, as it is there, ready for use when the demand arises. Possible demand will come from new Internet use, accommodating multiple identities with multiple IP addresses. Both protocols are expected to co-exist for a considerable amount of time.

However, the slow uptake will have consequences for the availability of free IPv4 addresses, which are now expected to run out in 2010-2011. The early adopters will still have sufficient addresses available to grow the Internet, as there still is considerable slack in reusing old addresses, but eventually a price will need to be paid, which will likely adversely affect developing countries and bottom up innovation/content production. This can lead to alternative solutions and potentially a new divide – endangering the global nature of the Internet - as 'the developed world' will switch to IPv6.

How the transition will take place and what the impacts will be is still largely unknown. For a smooth transition, scenarios would need to be developed urgently and governments need to actively promote the uptake of IPv6 and take a leading role.

Investment in broadband infrastructures and availability of spectrum

Investment in infrastructure upgrades and innovations may be hampered by the fact that the benefits do not (always) accrue with the same stakeholders that make the investments. Therefore, calls can be heard from (incumbent) businesses to allow limited monopoly rents on infrastructure to recoup the investments and allow for innovations. The argument is also heard that the infrastructure is a 'commons' and should be the responsibility of public authorities. There is no proof in these statements as the companies are actually still making profitable investments in infrastructure.

Users are becoming more active players; actually developing and owning parts of network connections. Experiments with such user-led ownership are ongoing and look promising; however there are issues for collective decision making processes.

Finally the current capacity of the broadband infrastructure is insufficient to deal with the new challenges created by the 'Internet of things', converging media technologies and platforms, user generated content, gaming and the growth of other bandwidth intensive applications. More bandwidth needs to be freed up and networks need to be upgraded to cope with the expected increase in traffic over the Internet. For specific purposes dedicated private networks will remain necessary; e.g. for emergency services. These networks could also be used for specific intensive purposes like science. This might help to alleviate pressure on the public network.

Interoperability

Today applications and tools suffer from failure, in particular in interaction with other applications and tools, as interoperability is seldom seamless, even if supported across platforms, in general. Some Digital Rights Management (DRM) applications are specifically made to avoid exchange and/or sharing across platforms, or even between users. An example is the chip in a DVD player that "protects" the region code. This prevents a Digital Video Disc (DVD) bought in the USA from being played back on a DVD system in a different region (e.g. Far East or Europe). Whereas "investment protection" as such has often been seen as a good thing (as it stimulates investment) at the same time measures may be limiting use for consumers and holding back development of new applications. Openness is also threatened by governments that block content as trade interference or to control free media and freedom of expression.

Fairness of network use

Much existing governance is based on roles and structures inherited from prior generations of technology. In those settings, it was reasonable to assume that businesses related to end-users as customers, and to workers as suppliers of (trained) labour. It was also reasonable (if not always correct) to assume that individual behaviour could respond more readily than institutional or contractual relationships, and to believe in certain asymmetries of information (e.g. that businesses knew more about the salient characteristics of the goods and services they offered than their customers did).

Many of these assumptions have been undermined by recent developments, and with them the comforting certainty that current arrangements will lead to optimal results. Of particular interest is the relation of the public (government), private (business) and civil (personal) domains. In one model that persists today in many countries, regulators constrain large businesses in order to restrain the exercise of market power. But in a changing world, it is not always obvious how this should be done. Regulation is costly and burdensome, and expensive or inflexible regulation may cause its own (more serious) distortions.

Despite changes in technology that seem to remove the natural monopoly argument for large telecom providers, for instance, in many countries dominant telecom companies persist, involved in long-term relationships with large monolithic regulators. These problems have been addressed through a variety of initiatives, including: the development of converged or realigned regulators (e.g. in Germany, the Netherlands and the UK); the 'Better Regulation' agenda with its emphasis on burden reduction and the need to consider non-regulation, de-regulation and other alternatives to regulation; and the development of more-effective 'incentive regulation' approaches.

Discrimination in speed and quality of service and price between different forms of traffic over the network should be allowed, based on the value, and the nature of the content, as long as the discrimination is transparent and not ant-competitive. It must be noted that different quality of service standards may be applied without the users being aware (slowing down traffic). Transparency allows users to make a well argued trade-off between price and functionality. Government should define what discrimination is acceptable and on what grounds, and make sure that these rules are effectively enforced.

However, in practice it proves difficult to monitor and enforce the behaviour of ISPs, thus there is a risk that ISPs will play along in order to 'buy' regulatory forbearance or co-opt the government's aid in deterring entry, imposing market discipline and controlling customer choice. On the other hand, where joint reputation effects are strong (e.g. the 'warm glow' of filtering content which all agree is bad) or where incentives to break self-regulatory discipline are strong, selfish incentives can reinforce rather than undermine social interests in improved filtering.

Universal service and the role of government

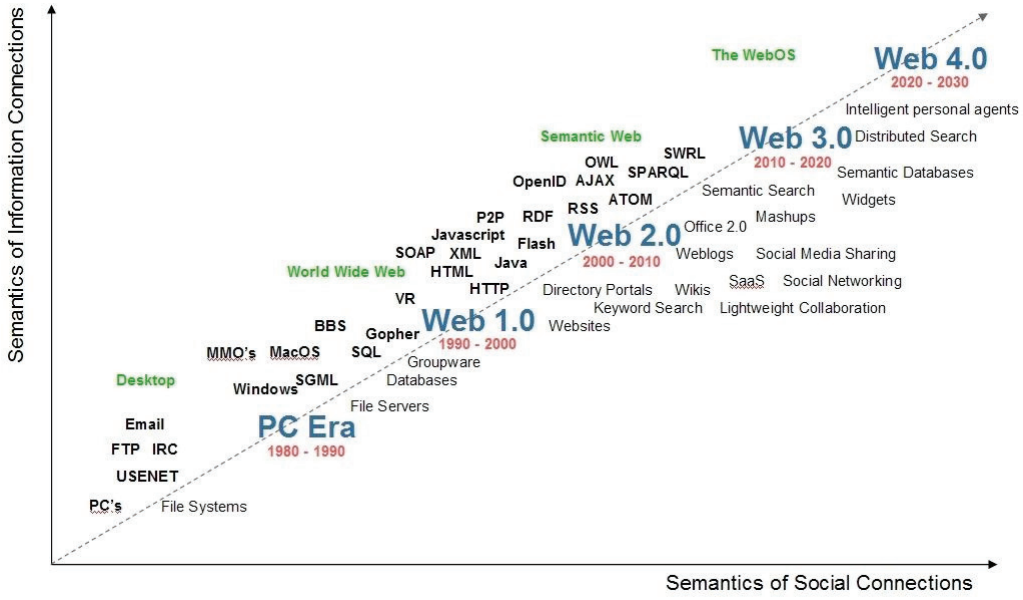
The provision of universal service, public infrastructures, and the protection of service quality used to be enforced by regulatory means. This approach is increasingly difficult, as new players are continuously entering the game and new technologies and infrastructures are deployed. Such objectives can often be provided more efficiently by suitably-implemented competition than by command-and-control, which suggests that greater use could be made of 'pay-or-play' public service obligations, 'use it or lose it' assignments of licenses and exclusive rights to operate and even a greater use of 'mechanism deregulation' – for instance, using suitable auctions[25] to establish access prices, commission services, choose standards, etc. In essence, these new roles have government acting as the agent of the economy; regulating where and to the extent necessary, providing encouragement to the identification and realisation of mutual gains and otherwise reducing its presence and institutional persistence.

[25] e.g. menu auctions in which bidders communicate about the impact on them of other bidders' 'winning' (which potentially takes externalities into account), share and in-kind auctions in which bidders offer arrangements for developing and sharing wider benefits rather than fixed sums of money and package auctions in which the appropriate scale, scope and duration of rights and public roles are decided simultaneously with the identity of winners and contractual terms.

Theme 2: Socio-economic dimension: Fostering creativity in the way we connect, work, make money and live.

Open, supportive environments and new collaborative innovation networks

The Internet and developments dubbed as Web 2.0 and 'Wikinomics'[26] are only just emerging and already having important impacts. It is important to realize that we are only at the start of the maturity curve and important and accelerated development still lies ahead. This is especially so in the emergence of virtual worlds, geo-spatial services and the deployment, use and impact of social networking applications. Further along more intelligent networks, devices and objects interconnecting and communicating among each other will be combined with far greater search capacity and artificial intelligence as we move toward the Internet of things and the Semantic Web. According to Tapscott[27], companies of the future can only be successful if they adopt the new and collective ways of operating: "Leaders must think differently about how to compete and be profitable, and embrace a new art and science of collaboration we call wikinomics."



SOURCE: Radar Networks and Nova Spivack, 2007

Figure A1.1: Semantic Map

[26] Term cornered by Don Tapscott in Wikinomics : How Mass Collaboration Changes Everything (2006)

[27] Tapscott, D. and A. Williams (2006) *Wikinomics : How Mass Collaboration Changes Everything* New York: Penguin Group

Figure A1.1 illustrates the ongoing dynamics in relation to technology, applications and architectures. The new paradigm referred to by Tapscott and Williams is largely driven by the production capabilities of users who do not necessarily seek monetary reward or remuneration - whilst underlining that financial stimuli can be very useful in encouraging collaborative approaches. To capture the outcomes of these activities various terms have been coined, such as "user generated content" or "user-created content". Creating user-created content (UCC) (the term used by the OECD) has become popular among younger generations, who share personal information and media, such as photos, videos and blogs (see figure A1.1). Websites such as Facebook and YouTube have become important enough to trigger relatively large investments with the prospect of substantial revenues.

Recently, the increase in UCC has further stimulated the development of business models which aim to generate revenue from UCC sites. As these developments are in their early stages definitive or well established models do not exist, however, the OECD lists several new business models aimed to monetise UCC[28]:

- *Voluntary donations*: websites employ the option for users to make voluntary donations.
- *Charging viewers for services*: possible via
    - *Pay-per-item model*: users make payments for the pieces of content they wish to access.
    - *Subscription model*: users subscribe to a particular service and can then access content. However, it is noted this option is rarely used.
- *Advertising-based modes*: the audience is monetised via advertising. This is seen as a particularly significant driver of UCC, as they enable contents to remain free, while revenues are generated.
- *Licensing of content and technology to third parties*: in this model UCC is made available for other platforms, as content is licensed to third parties. In this model a revenue sharing model may exist between the content creator and the UCC site, however this is not necessary.
- *Selling goods and services to community*: the users of UCC sites become the audience of marketing for products. Products marketed can stem from both the site itself or from third parties.

In the future it is expected these models will further develop and new models will arise. Already many of the most visited websites online are UCC sites as shown in Table A1.1. below. It should not come as a surprise that large Internet corporations such as Google, Verizon and Microsoft have all invested in such sites.

[28] OECD (2007) *Participative Web and User-created Content: WEB 2.0, WIKIS And Social Networking*, Paris: OECD

Table A1.1: Websites Online Market Share US October 2007

Rank	Website	Market Share
1	www.google.com	5.14%
2	mail.yahoo.com	4.99%
3	www.myspace.com	4.88%
4	www.yahoo.com	3.95%
5	mail.live.com	2.08%
6	www.ebay.com	1.83%
7	search.yahoo.com	1.66%
8	www.msn.com	1.52%
9	www.facebook.com	0.96%
10	www.youtube.com	0.69%
11	Search.msn.com	0.53%
12	Images.google.com	0.51%
13	www.gmail.com	0.48%
14	www.wikipedia.org	0.47%
15	www.hotmail.com	0.39%
16	My.yahoo.com	0.38%
17	mail.aol.com	0.38%
18	www.pogo.com	0.35%
19	address.yahoo.com	0.34%
20	www.ebaymotors.com	0.33%

SOURCE: Hitwise.com

The 2006 growth figures in Table A1.2 show the emerging trend and the comparison with 2007 demonstrates the impact of UGC on WWW traffic.

Thus, the quick expansion of UCC has attracted the interest of businesses. Economic and social activity increasingly overlap, where UCC, collaborative production, and customer created products are becoming increasingly popular.[29] Figure A1.2 illustrates the ratio of UCC producers to Internet users in the EU.

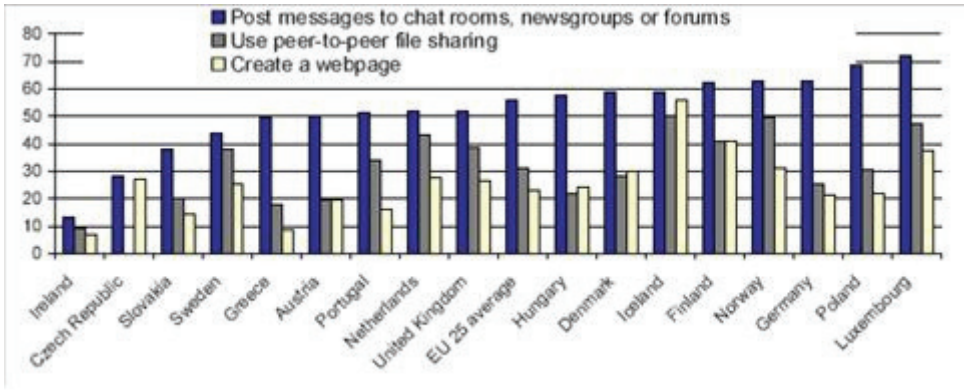
[29] OECD (2007) *Participative Web and User-created Content: WEB 2.0, WIKIS And Social Networking*, Paris: OECD

Table A1.2 Fastest growing web sites among US at-home and at-work Internet users, July 2006

Firm	Type of Internet Services	Number of unique visitors (millions)	% growth of unique users July 2005 - July 2006
HSBC	Bank	6.4	394
Sonic Solutions	Provider of digital media software	3.7	241
Associated Press	Press agency	9.7	234
ImageShack	Image hosting site	7.7	233
Heavy.com	Video sharing site	3	213
Flickr	Photo sharing site	6.3	201
ARTIST Direct	Online music platform	3.2	185
Partypoker.com	Online gambling site	6	184
MySpace	Social network site	46	183
Wikipedia	Online community project	29.2	181

SOURCE: Nielsen//NetRatings, July 2006, www.nielsen-netratings.com/pr/PR_060810.PDF. Sites in bold are relevant to UCC

Businesses loosen control to give way to (mass-) collaboration and sharing in order to improve and co-create new products. Secrecy and protection are slowly being replaced by transparency to foster innovation and development.[30] Collective operations therefore, seem to give rise to the creation of new value chains and business models.



SOURCE: OECD 2007

Figure A1.2 : User-created content creators in the EU as a % of Internet users, 2005, age group 16-24 years

The openness of mass-collaboration and the transparency of UCC production give rise to new value chains in the creation of media. Compared to traditional offline media publishing value chains, the UCC value chain is less static and open to almost all who have

[30] Tapscott, D. and A. Williams (2006) *Wikinomics : How Mass Collaboration Changes Everything* New York: Penguin Group

Internet access. Input is now provided by all, to be judged by all. In this process traditional gatekeepers of quality assurance are being replaced by the judgment of the masses, hence popular content follows from the preference of users[31].

The participation of a big online audience can further affect the manner in which products are designed, tested and eventually produced. New designs can be tested online, perhaps in accessible virtual reality environments, to allow for the creative input of the masses. In this sense design could become a type of social experiment which is not dependent anymore on the few, yet aims to benefit from the creative potential of the available collective. This also has spin offs in marketing, as the collective engagement carries its own message.

Furthermore, means of production change as products are developed by large groups, each member adding a bit to the larger product. The classic example is the development of the open source operating system Linux, which has been professionalized and developed by input from collectives. Those making a contribution often do not seek remuneration, which might give rise to the development of a new business model on the basis of sharing without self-interest. Value creation activities such as open source software and others based on social networking acquire a new "karma"-like dimension. Questions can arise however, regarding property rights and the control of intellectual property, as it is unclear who owns the newly created products, and who might possibly profit from their commercial use. The role of government is often to support innovation, yet also to ensure control over IPR. Thus, in the new collective environment, these two tasks might prove difficult, as control over property rights could harm the collective innovative input.

The business models in the new connected Internet economy will have to be more open and flexible. With the cost of transactions and collaboration diminishing, the justification for large scale organizations with big R&D departments and corporate support is slowly unravelling. SME and individuals now have access to the computing power, the connectivity and services that once was reserved for large organisations. Their flexibility and agility will threaten large incumbent enterprises, which are tied up in legacy systems and are more likely to defend obsolete business models. Looser networks of independent experts acting like markets are likely to emerge[32]. Mass collaboration will be able to develop new products faster and better adjusted to meet market demands. Moreover, the products of the future are likely to be more like services, as the 'things' start connecting and communicating and performance of devices becomes largely dependent on embedded ICT.

Intellectual property protection and scientific sharing

The ease with which IPR can be circumvented in the Internet economy creates particular problems for the flow of invention, innovation and investment (in RTD as well as in productive capacity tied to specific intellectual property). If intellectual property is too easy to copy, or if users gain access to the fruits of costly RTD and innovation activities without

[31] OECD (2007) *Participative Web and User-created Content: WEB 2.0, WIKIS And Social Networking*, Paris: OECD

[32] Malone (2004) The Future of Work: How the New Order of Business Will Shape Your Organization, Your Management Style, and Your Life Boston: Harvard Business School Press

paying, the incentives to undertake such investments in the first place are undermined. Moreover, firms may seek to protect their investments and earn 'just returns' in other ways – e.g. by rapid changes, strategic structuring of IPR and/or DRM practices that impose performance, reliability and quality burdens on customers or the system as a whole. In this way, the rents (excess returns) to invention are converted into social costs, rather than being shared throughout the economy. A traditional answer would be to enhance the enforceability of IPR through technical and legal means. But these are not costless, and in many cases social value is created through the clustering of innovations rather than through 'killer ideas.' In such cases, innovation has at least a partial public good character, and intellectual rights regimes based on individual, exclusive and transferable property rights may need to be replaced by more variable 'rule of reason' approaches that allow variation in the scope, extent and duration of rights, or which incorporate 'options' to be negotiated after subsequent innovation has materialised.

A second point is that the exercise of traditional IPR monopoly power may not be optimal in the specific circumstances of the Internet. Three examples illustrate the point. The first involves interoperability – if the value of a good or service increases as more people use it, it may be profit-maximising to retain strong IPR protections, but to enforce them only on high-value, low-elasticity users – the 'violations' by low-value users sacrifice relatively little revenue but expand the user base and thus the willingness to pay of high-value (e.g. corporate) users who *will* abide by IPR rules. The second concerns the production of complementary innovations – a profit maximising inventor will wish to make access to his innovation freely available to producers of complementary goods in order to reinforce a critical mass and a *de facto* standard. To some degree, this leads to tipping and the risk of excessive volatility (as innovators rush to the new potential market leader) or excess inertia (as firms avoid the risk of stranded investments in an obsolete technology), but the benefits of complementarity and the possibility to negotiate or trade around these risks provide strong arguments for more flexible arrangements – again, with a range of negotiable duration, bundling and strength to avoid the consequences of a one-size-fits-all system. Finally, the importance of user-generated innovation and other sources of inventive activity not motivated by monetised profits suggests that the use of markets to motivate and control innovation has its limits, and thus that Creative Commons, General Public Licence (GPL), compulsory licensing and 'social IPR' all have roles to play.

The key point is that reformed IPR rules can encourage not only the flow of new ideas, but:

- new ideas offering a higher proportion of societal (as compared to commercial) returns
- innovations that are more 'open' to subsequent or parallel development
- situations in which the struggle for control of the 'market for ideas' does not subvert competition in the 'market for goods and services' and
- IPR arrangements that are better-suited to the resolution of uncertainty during the life-cycle of innovation and to the partnership of commercial and non-commercial (research, public sector and civil society) entities.

Social Impacts: ICT skills and digital and media literacy

New communication technologies have allowed people to communicate almost anywhere, anytime. Family and friends are now able to communicate with each other at different ends of the world, bringing people closer than before. Very few elements of social life have remained untouched by the Internet and it can only be assumed that the further development of these technologies will affect our daily social life to an even larger extent. Various nested aspects of social life (from institutions to values) are thought to be in balance in stable societies, so that a disruption at one level can trigger a wider unravelling of the social fabric. This was noted in earlier times for the factory system that took work out of the family context; the automobile, which dispersed the centre of economic activity and social contact away from local communities; and electricity, which disrupted day/night social rhythms and labour relationships. To understand the wider impact of the Internet on society it is necessary to look at the social changes brought about by the Internet in our daily lives.

We see the facilitation of communities and identities. Many social groups (re)invent identities due to renewed communication of group members. Cultural groups re-establish group identities while simultaneously new identities are formed on the basis of communication over the Internet[33]. The global nature of the Internet allows formerly unconnected people with similar interests find each other, resulting in new and wide ranging interest groups. Of course these opportunities are offered to those with ideas in opposition to those prevalent in society. In this way the Internet can also facilitate the organisation of activists, criminals, paedophiles etc.

Virtual worlds, from online games to Second Life, open new opportunities of online social interaction; new social skills can be learned and new interactions experienced. eCommerce is further extended to virtual worlds where with real money virtual products are purchased in a virtual market place. Similarly virtual currency can be exchanged in the real world. Virtual worlds can spur creativity and imagination as new ideas are easily exchanged via virtual identities, thereby providing new inputs for UCC. Thus social learning within virtual worlds could contribute to the development of human and social capital, which could benefit the collective production capabilities of the group.

However, virtual worlds can also impact negatively upon daily social and individual life. People can become detached and withdrawn from their physical environment, preferring to solely engage in virtual interaction. Virtual assets or possessions that may hold value in a virtual world may become the targets of real world crime. Furthermore, as virtual worlds offer a platform of experimentation of new ideas, violent or disruptive ideas might also arise and influence people in virtual worlds. This again calls into question the role governments could (or to some should) play in the regulation of such alternative realities. Is policing required, or should providers of virtual worlds and associated identities ensure safety of participants?[34] On the global scale at which virtual worlds are currently being

[33] Bargh, J.A. and K.Y.A. McKenna (2004) "The Internet and Social Life" *Annual Revue of Psychology* Volume 55 pp.573-590

[34] Lastowka & Hunter (2004) "The Laws of the Virtual Worlds", *California Law Review;* Balkin (2004) "Virtual Liberty: Freedom to Design and Freedom to Play in Virtual Worlds" *Virginia Law*

developed, it seems inevitable that without the involvement of multiple stakeholders little can be achieved.

The Internet and ubiquitous connectivity have empowered the individual in all his/her roles as a citizen, a consumer, a pupil, a patient, a creator of content, a communicator, etc. It has allowed much greater civic engagement and participation, as information is readily available and increased transparency allows real time involvement with democratic decision making processes. The Internet also enables the rabid mobilisation of mass movements of people for social action.

Moreover, now many individuals are equipped with the ubiquitous camera-phone, ordinary people have turned into witnesses, journalists and documentary makers. The Internet provides a publishing tool to send images and messages to global audiences. Whilst there is this huge increase in the intake of information and the explosion of individual expression, there is no parallel formal quality screening and filtering mechanism, like editing boards, professional ethics, etc. Peering and ranking are becoming the mechanisms to establish the credibility and quality of a (re)source, or the relevance and accuracy of a story; and the difference between fact and opinion; truth and fiction.

Theme 3: Reliable use and common Trust: strengthening confidence and security

Usage of the Internet respects fundamental rights and freedoms (dealing with risks)

Having become dependant on the normal functioning of the Internet in so many ways, it is key to ensure common trust in its use. The rapid uptake of Internet usage for all kind of purposes (chatting, networking, shopping, accessing information, etc.) is the best and perhaps the only reliable source that demonstrates the existence of "common trust." People engage in transactions and communication on the Internet, because, taking account of the risks, they see a benefit.

Nobody thinks the Internet is perfect, or ever will be perfect. Yet the Internet has become an important part of our lives, and we expect this part to continue to grow, both for new groups of people, and in terms of pervasiveness for those already using it. Trust, when justified, is an important factor to reduce transaction costs, both in the economy but also in social life. It builds on available, dependable networks, secure systems with reliable information and assurances of reliability.

The Internet was never built for the wide range of purposes that it has in our daily lives today, nor was it meant to be so pervasive. As more applications are likely to be identified and the pervasive impact on our daily life is expected to grow, it is important to reflect this

---

Review, Vol. 90, pp. 2043-2098.; Crawford & Rutter (2006) "Playing the Game: Performance in Digital Game Audiences", in: Gray, Sandvoss & Harrington (eds) *Fandom: Identities and Communities in a Mediated World* New York: New York University Press

in actions to improve the reliability and security of the Internet and its use in such a way that common trust is encouraged.

As with all technologies, and infrastructures, the Internet is not good or bad in itself: it is the way we use it. The design of the Internet as well as the "rules of behaviour" and, of course, enforcement of those rules are key in supporting "good" use and avoiding misuse. If the intensive use of the Internet is to continue trust levels must remain high. It is therefore in the interests of all stakeholders to ensure a safe and secure Internet environment which ensures sufficient levels of trust with users.

Several trade-offs can be identified that are directly relevant to the "trust" issue:

1. Security vs. convenience and costs
2. Privacy vs. security and user friendliness

Security measures cost money, and cause delay in systems. Therefore there is an incentive to keep them as low as possible, although it is clear that too little security is likely to result in costs resulting from damage. The risk of damage is considered when investments are planned into delivering the security of systems. Whereas this leads to individual risk assessments (based on personal risk profiles) at the general level of "society" it is more difficult to assess what the risks are, and to allocate costs (of investments) and benefits (of reduced risk for damage). Transparency and risk awareness are seen as key drivers to get this right: those parties benefiting most from risk reduction (for instance eCommerce companies) will be most inclined to invest in security measures, as the experience of security enhances trust amongst their customer base.

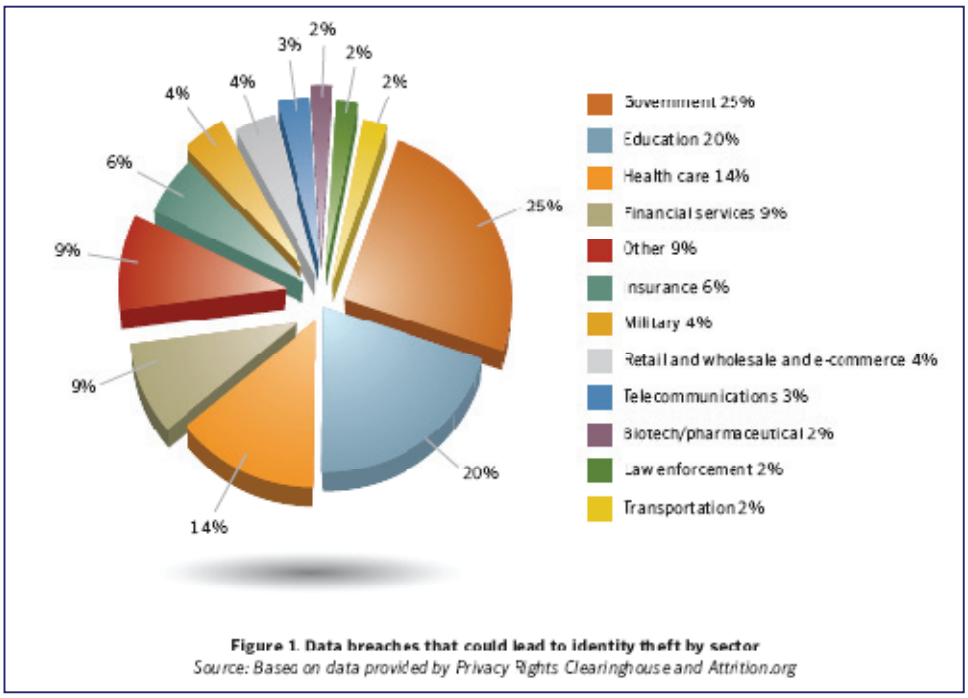
In terms of user convenience, it is clear that security measures make life more difficult (the user has to remember many PIN codes or passwords, and repeatedly go through the effort of identifying themselves to systems). With arms full of Christmas presents, it would be so much easier to just stand in front of your door to gain access to your home rather than turning a key; nevertheless people accept a certain level of inconvenience in order to reduce the risk of people just walking in. Again, which level of discomfort or inconvenience is acceptable for obtaining a certain level of security is very much dependent on culture and personal (risk) preferences. It is also exactly for this reason that we accept that the State acts to enforce the law and ensure security.

Protection of digital identities, personal data and privacy of individuals

Privacy is not a goal in itself rather the right to privacy is a means to ensure freedom of choice, which stops at the moment that choice would adversely affect others in ways that are not acceptable. A specific challenge is that everybody would want their privacy and access to their personal data and traffic on whatever they do on the Internet to be protected. However, at the same time the Internet is used for illegal and dangerous purposes, ranging from paedophilia, use as a tool of terrorists and organised crime, and/or distribution of viruses and other forms of misuse. In order to be able to investigate and pursue people and organisations involved in such activities, there is a need to be able to track and trace information streams. A key concern arises that with access to such information, oversight of the law enforcement and intelligence services becomes a critical issue. Who would police the police, in particular in a global environment like the Internet?

Less dramatic but more dependent on personal preferences and choice (anybody may opt out, without detriment to others) is the trade-off between privacy and convenience. Having access to certain personal information can help provide a service that is more made to measure or personalised, ranging from not having to provide all kinds of administrative data repeatedly, to presenting you your coffee just the way like it, without having to ask!

Anonymity and identity are key issues when talking about privacy. As the abundance of data is structured via its connection to identities, it is clear that identities are key assets. Already today identify theft causes problems. Figure A1.3 below shows in which sectors in the United States concerns about identity theft are most heightened.



SOURCE: Privacy Rights Clearinghouse and Attrition.org

Figure A1.3: Data Breaches

It is now common knowledge there is no anonymity in the Internet world. Everything that is ever said about a person can be stored anywhere and can 'pop up' at any time. This means that, for instance, radical or alternative opinions expressed on the Internet may haunt us even after retirement, but maybe more importantly when we are in pursuit of new jobs or in the public eye. While privacy is one of the fundamental rights[35] supported by legislation that requires withdrawal and/or rectification of personal information when demanded by the data subject, the nature of the Internet itself and electronic data per se may not result in this happening due to copies of such information residing on other third-

[35] See for instance chapter 7 and 8 of the European Charter of Fundamental Rights http://www.europarl.europa.eu/charter/pdf/text_en.pdf

party databases, search engines, etc. Such loose shreds of information may lead to misperceptions and erroneous value judgements if the supporting context is missing or false. Not only will it be increasingly difficult to stay anonymous, but there is a risk that the available data will be taken out of context or be easily (maliciously) manipulated.

Trust and the prevention of malicious activity online

Breaches of privacy can undermine a critical condition for building inter-personal relationships and enabling transactions in an uncertain environment: the existence of *trust*. But as the research from Unisys (Box A1.1) proves, privacy is not the only factor at work in building or abusing trust.

Trust is an immensely important component of any online transaction– as it is off line. There are a wide range of transactions including: Business-to-Business; Business-to-Customer; amongst individuals via auction sites etc. and in each transaction trust will influence whether parties engage in transactions or not. Hence ensuring sufficient trust is vital for both business as well as customers. Fraudulent behaviour online damages trust relations and can reduce online economic activities. It is thus in the interest of business, customers and government to ensure a safe and trustworthy online environment which is conducive of online transactions.[36]

Box A1.1

Findings from Unisys research on Trust.

Trusted enterprise research:

- **Trust is vital to the success of any enterprise and administration:**- 53% recognize that privacy protection builds trust- 73% believe not protecting privacy erodes trust
- **Trust & loyalty in financial services: Consumers would switch to another bank offering better protections for personal information** (Europe 68%,UK 87%, US 75%).
- For consumers **prime trust building factor** in Germany is product quality (68%) and in UK respect for customers (93%).
- **Most trust eroding factor** is unethical business practices (Germany 74%, US90%).
- **Least trusted industry segment** in Germany is energy, in the US insurance, and in UK entertainment & media.

Security Index:

- **Fraudulent credit card use and unauthorized access to information are priority concerns for Europeans – 81% (**top concern in Europe (55% significantly concerned)).

[36] Putnam (1993). *Making Democracy Work: Civic Traditions in Modern Italy* Princeton University Press; Sztompka. (1999) *Trust. A Sociological Theory* Cambridge, CUP; Gavish & Tucci (2006) "Fraudulent auctions on the Internet" Electron Commerce Res Vol. 6, pp. 127–140; from RAND Europe Cyber-Trust and Crime Prevention Scenarios (2005)

- **Misuse of personal information is another major concern for 81% of respondents** (50% significantly worried).
- **Only 35% of Europeans are very concerned about computer security and the threats of viruses, spyware or spam.**
- **Only 30% of Europeans are significantly concerned about shopping online** (35% not concerned at all).

Germans are seriously concerned about identity theft and credit card fraud (70%), **computer security** (60%), **and security of online shopping and banking** (44%).

Source: Unisys 2007

A determining factor in the use of e-commerce is the feeling and perception of security. The more secure and trustworthy a service, then the more likely that it will be used. Thus in order not to lose customers it appears crucial for providers of Internet–based services to provide secure and safe services which instil trust in the perception of users. Reputation building, the signalling of trust and reliability is therefore important for e-businesses which wish to maintain and increase transactions.[37]

There are certain measures that could be considered in order to improve reliable use and common trust on the Internet:

- Provision of reliable end-to-end connectivity by tunnelling, thus ensuring there is no misunderstanding about who is talking with whom, and that the connection can only be used for the purpose it was set up for.
- Active Internet policing, pursuing perpetrators and preventing crime, within a clear meta-structure that "polices the police" and avoids abuse of power by security services.
- Identity theft is a reality, and needs to be actively addressed, yet the idea of being able to provide full prevention forever is an illusion. In case of identity theft measures need to be in place to prevent, reduce and recover damage to parties. These measures should include active use of privacy enhancing measures and technologies, combined with a more conscious way of providing only the information from a person, with established consent that is needed for the specific purpose. Measures to ensure this range from assuming liability for parties storing and processing personal data, to governments taking the lead.
- A clear connection is required between recognising security risks and apportioning responsibility and liability for dealing with such risks. By insertion of default "open" technologies and protocols in the Internet this may become possible without harming the wider openness of the Internet.

[37] Malhotra, Kim & Agarwal (2004) "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model" *Information Systems Research* Vol. 15, No. 4, pp. 336-355; Gavish & Tucci (2006) "Fraudulent auctions on the Internet" Electron Commerce Res Vol. 6, pp. 127–140; Kima, Song, Braynov, Rao (2005) "A multidimensional trust formation model in B-to-C e-commerce: a conceptual framework and content analyses of academia/ practitioner perspectives" *Decision Support Systems*, Vol. 40, pp.143-165

In order to avoid disappointments (and thus reduction in "common trust") addressing the information asymmetry as regards risk is key. This can be achieved by raising awareness. When the consumer/citizen becomes aware of her or his risks, she/he can make an informed choice. Consumers need to know where to find trustworthy information. Risk is as such not a bad thing, as long as informed choice is possible. Instead, the focus should be much more on "opportunity".

Governments could assume leadership in this: as major players in the Internet economy they can set examples of good practice and invest in measures that improve the overall reliability of the Internet (within their region or even beyond). Furthermore governments can play a catalytic role by stimulating and supporting "learning from experience" by sharing best practice and experience, and by adapting student curricula to include awareness of information vulnerabilities and choices to reduce those risks. It is important to recognise that sometimes it is not sufficient just to rely on the Internet as a communication medium. Sometimes confirmation via telephone or even in person may be necessary to keep the risks of mistakes or abuse within an acceptable range e.g. in the case of online only auctions between consumers. Governments have a special position in this respect because they are driven to conduct transactions over the Internet with any company or citizen. Thus for them it is a key priority to provide a safe and yet very easy and accessible e-environment, setting standards for others.

Robustness of the Internet

The openness of the Internet as a network of networks is its strength and should be guarded as a key feature. Security should be dealt with at the edges (at the end-users, in the applications). Encryption would effectively allow secure data exchange over public networks, but if security is an essential feature than the application should use a dedicated private network (e.g. with SIS II, GÉANT and some banking services). There are no comparable service level agreements for public networks.

Spam remains a (growing) problem. It is prevalent at the application layer and is inherent to openness of the network. The Spam business model is built on low cost of mass dissemination and the reply of a small minority of recipients. The only solution is to raise awareness of the consequence of responding. There is also a development aspect to Spam as it causes disproportionate disruption to users that cannot afford the latest filters and anti-spam software.

When assessing the security of the network the nature of handheld devices must also be considered. They should not be too intelligent to avoid the risk of compromising security of the network. However, 'dumb; devices may now form an intelligent network in and of themselves. There is no equivalent transparency to real life security in cyber space. Consumers do not know what security is provided by ISPs. Overall awareness of the risks and effective protection is low at many levels. This will only increase with the emergence of the Internet of things and the Semantic Web. The complexity of data exchange between interconnected objects, people and intelligent devices makes it impossible to assess personal or system risk, let alone warn users of the potential risks.

Theme 4: Internet Governance: ensure that the Internet economy is truly global

Net neutrality and global access

The Internet has traditionally been a self-regulated and interconnected global network of institutions driven by its educational and later global business priorities. Innovators and their companies, funded and fostered by generally supportive market-led governments have created co- or self-regulatory institutions or compacts. Examples include the various Internet Service Provider Associations across Europe and increasingly in other territories. However, with the global consumer adoption of broadband Internet, with a billion users and over 250 million broadband connections, such institutions properly need to consider the social and economic rights and responsibilities of consumers at national, regional (including European Union) and global levels. The involvement of consumer-citizens on a more legitimised and consensual level than industry self-regulation as classically defined in ICT sectors – notably technical standard setting activity – is still a novel approach.

ISPs may be forced or self-impose a role as filters on information provided by content providers to end-users, and between networks of producers and consumers, including the important new categories of user-producers in 'Web 2.0', in particular for content that is widely regarded as illegal and/or harmful. ISPs' decisions to invest in the consumer's Internet connectivity include the consideration of whether the network is offered as:

- a non-discriminating wholesale or retail network,
- or a 'walled garden', as in mobile networks (e.g. the 'Vodafone Live' portal).

There are lots of types of 'walled garden', but in general they have the feature of enabling preferential access to content partners, and keeping the 'walls' around their content high enough to keep out undesirable content. In policy terms, the question is whether those barriers are maintained for good network security and technological efficiency aims, or for economic discrimination, or even for content filtering for end user preferences (e.g. to make only content labelled as suitable for families available as with some AOL filtering rules). These reasons overlap, making the legal and regulatory task of deciding on suitable and unjustifiable discrimination extremely difficult.

The potential exists for future technologies of filtering to substantially change the balance of power between nation states and individual users over the global Internet. Before allowing states to partition the global information resource in this way, it is a relevant question to ask whether this solution to existing harms might be to damage the medium's innovative capacity. However it is important when asking ISPs to block and therefore censor content to "be careful what you ask for". [38]

We might add, be careful that all stakeholders are engaged in the discussion to encourage legitimacy in the final decision and its observance. There should be greater citizen/ consumer participation in policy making, whether it be hard or soft in this area, and

greater capacity for multi-stakeholder governance. Besides different stakeholders, Internet governance is also dispersed at various levels, from the infrastructure to the online services[39]. The question thus arises as to which bodies are most appropriate to govern what parts of the Internet.

Cross border cooperation in consumer protection, spam, privacy and cyber security

Governments have an obligation to protect their citizens; however, in the virtual world of the Internet, protection, regulation and legislation are far from straightforward. Every single law can inflict upon the open character of the Internet environment and could harm information sharing. Furthermore, the borders of the Internet do not collide with national borders which pose further limitations upon national jurisdictions. The role of national governments in the future of Internet regulation is therefore an interesting topic.

Novel experimentation has been taking place over the roles of companies, governments and consumers/citizens in debates around responsibility and the Internet. It provides a very influential framework for examining the future developing role of regulation. Hoffman explains that Internet governance: "can be understood as an open-ended, collective process of searching which aims to fill a global 'regulatory void' both conceptually and institutionally in a legitimate way. This void arose because the principle of sovereignty, which was an essential component in international regulation of the telephone network, has not been carried over to the Internet." MacLean states: "a complex and confusing array of local activities take place without any overall coherence or top-down coordination of the kind formerly provided by the United Nations agency".[40]

The United Nations Secretary-General in 2004 established a Working Group on Internet Governance (WGIG) to provide some clarification of the term and the public policy issues that are relevant in this context. It reported at the second World Summit on the Information Society (United Nations (2005)). Its concerns are largely technical in character, yet its central concern is absolutely clear and non-technical: Internet governance is an inter-governmental, technical and market-led phenomenon, but also (and critically) involves the Internet user, as demonstrated in the composition of the WGIG itself. It has been extended in the work of the Internet Governance Forum (IGF) which first met in Athens in 2006, in Rio de Janerio in 2007, and then meets in India in 2008.

Such co- and self-regulation experiments have been extended, in for instance the United Nations context through CONGO (the Conference of Non-Governmental Organisations), through the Domain Name System and ICANN (the Internet Corporation for Assigned Names and Numbers: Mueller 2002), and locally through for example the UK regulator Ofcom, which conducted a long-term study of such arrangements in 2007.

---

[39] Dutton and Peltu (2005) 'The Emerging Internet Governance Mosaic: Connecting the Pieces', OII Forum Discussion Paper, No. 5, Oxford: Oxford Internet Institute, University of Oxford

[40] MacLean (2004)

The United Nations is providing a more durable multi-stakeholder relationship in regard to Internet governance. Its call for informal multi-stakeholder arrangements beyond the traditions of the ECOSOC (Economic and Social Council) arrangements that dominate post-1945 institutions such as the European Union and United Nations, is a novel and fascinating attempt to achieve real global dialogue around responsibilities in the "Information Society", and may be a significant new governance paradigm in the coming years.

The three main governance issues that emerge at this time are the value of multi-stakeholder approaches; the relevance and challenges for self- and co-regulation and the overall global Internet governance structure.

Develop mechanisms to respond: multi-stakeholder approaches

Multi-stakeholder approaches have been struggling to be accepted by leading actors and institutions at national, regional and multilateral levels. As awareness grows that traditional approaches fail and that the involvement of key stakeholders in implementation and enforcement of policy objectives is unavoidable, such approaches are, however, becoming accepted. There are some inherent limitations that need be taken into account, most importantly:

- Multi-stakeholder approaches are still driven by personalities, which contain a high risk of discontinuity and limited institutional learning within the participating organisations and existing processes
- Openness to new stakeholders is not evident; risking to shut out emerging players and thus not capturing important new developments and/or diminishing the constituent basis of such approaches and thus their legitimacy
- Accountability and endorsement of outcomes
- Inefficiency, leading to high cost - in time and funds - to practitioners in order to influence decision making processes.

The application of multi-stakeholder approaches at global levels adds an additional layer of complexity, as the levels of acceptance of non-state actors' involvement is very different from country to country. Additionally, the quality of civil society organisation differs widely.

Multi-stakeholder approaches have to stand up against much stronger established organisations. To allow such approaches to mature and to make them more effective, there needs to be a better and more widely shared understanding of the mechanics of governance. Thus collective learning (e.g. WGIG) needs to be improved and also institutional knowledge and experience of participating organisations and individuals must be better captured as they are built up. In doing so the role of the engineer and technical knowledge must be given sufficient weight alongside legal, policy and other considerations. It is felt that among policymakers the awareness of the technical parameters is still largely insufficient, which affects the quality of the outcomes of policy making.

Governments should endorse existing multi-stakeholder mechanisms, to allow them to mature into effective approaches; by credentialing and legitimisation. This can also occur

at the level of organisations like the OECD. Government should also invest in educating policy-makers on technical, legal and economic dimensions. Another natural role for government would be the active and visible enforcement of the outcomes of multi-stakeholder processes.

Self-regulation and co-regulation

To complement traditional regulation where enforcement, monitoring and control by the public sector prove difficult or overly intrusive, the use of self-regulation and co-regulation has been explored.

For self-regulation to be effective and sustainable, it needs to be embedded in some regulated context. There must be some threat of regulation or at least some underlying 'hard' norms, thus effectively providing hybrid approaches dubbed co-regulation or 'compelled self-regulation (EC)' or even 'involuntary self-regulation'. With maturity it is often absorbed by this formal context.

Self-regulation has certain challenges. Typically legitimacy and effective enforcement are difficult, but so is accountability and defining the boundaries of reach. The impact on third parties is difficult to control; new ones that need to be included might slip through, as well as others that are affected without falling under the strict scope of the regime. There may be cases where the self-regulatory scheme is a mere façade to fend off the threat of full scale regulation, without providing the effective protection, policing, arbitration, and remedy for which they were set up.

Government plays an important role in enabling parties to self-regulate, and in endorsing self-regulatory schemes, as well as monitoring their effective and fair implementation and impact in practice. Only government can provide the legal embedding and when necessary the institutionalisation of self-regulatory approaches to ensure their sustainability for the benefit of the common good. The key for any action is to understand the way to link self interest and common interest. This can be achieved through design or evolution, and sometimes requires either rule-setting or light handed steering.

International Internet Governance

The Internet has developed into a global critical infrastructure, prompting governments across the globe to state their desire to have a say in the way it is governed. Moreover the Internet does not stop at geographic borders and national jurisdictions have proven incapable of effectively controlling its use. The global nature of the Internet implies that everyone is affected by everyone else's behaviour online: e.g. poor security in the developing world affects eCommerce in other parts; spam, fraud, cyber-crime which can affect all users may originate from countries with weak law enforcement capabilities and insufficient legal provisions. Conflicting values thus become apparent like the application of one notion of privacy outside of the cultural context.

In setting up the global governance of the Internet due attention must be given to good local governance, and must be explicit about certain issues e.g. transparency, accountability, multi-stakeholder involvement, exchange of good practice. It should

accommodate the diversity of user communities and also provide some consistency, standards and rules.

As the Internet and its role and use changes, its governance should be accommodating and flexible. Some of the issues that need to be taken into account to adjust to a changing Internet environment are:

- Focus on users
- Make clear what the value of governance is for the users
- Recognise emergence of new commons
- Prepare for the unknown, as we cannot foresee future developments
- Release public sector information to add to the value of the 'commons'

In the development of global governance structures the following principles of good governance could be applied[41]

Transparency	• Clear and well-defined rules which identify intended outcomes; • Simple and clear guidance notes for those applying the rules; • Clear and accessible internal channels of communication; • Clear, accessible guidance for consumers about what the scheme does and does not cover; • Published annual reports or equivalent, detailing financial performance, numbers, handling and outcomes of complaints etc.; • Independent dispute resolution procedures; • Clear delineation of roles within the organisation (e.g. a separate disciplinary committee).
Accountability	• Appropriate and properly used channels for consulting members; • Well publicised, quick and simple procedures for dealing with complaints from the public; • Well-publicised, fair and efficient appeals procedures both for members and consumers; • Access to independent arbitration or an ombudsman; • Transparent processes for appointing and removing governing bodies; • Lay representation on decision-making bodies to ensure balance between bringing expertise to bear and the need to challenge professional complacency; • Clear division between self-regulation and any body representing the industry's interests; • Mechanisms for reporting on activities to the wider public.
Targeting	• Clearly defined goals and objectives; • Performance indicators to measure effectiveness;

[41] The Principles of Good Regulation were first devised by the UK Better Regulation Task Force in 1997 at its foundation, and discussed in greater length in the 2006 report" Principles of Good Regulation" at: http://www.brc.gov.uk/upload/assets/www.brc.gov.uk/principlesleaflet.pdf

	• Priority given to addressing greatest risk of harm to consumers; • Extensive internal and external consultation on rules and codes of practice; • Regular reviews to assess whether the rules are necessary and effective.
Proportionality	• Mechanisms to impose meaningful sanctions on those who break the rules but not to disadvantage those that want to comply; • Procedures in place to allow government monitoring; • Procedures which ensure that good practice is not threatened by risk of disproportionate sanctions for relatively minor offences.
Consistency	• Rules that dovetail with other relevant rules and regulations; • Procedures to ensure that similar problems are resolved in similar ways.

Appendix B: Reference Bibliography

These sources were used at the various stages of the project, in particular for the horizon scan of the most relevant issues. They also contain the references noted in the discussion paper.

Acquisti & Gross (2006) “Imagined Communities: Awareness, Information; Sharing, and Privacy on the Facebook”, PET 2006

Allenby & Fink (2005) “Toward Inherently Secure and Resilient Societies” *Science* Vol. 309 pp. 1034 - 1036

Baker (2003) “National Security versus Civil Liberties” *Presidential Studies Quarterly* Vol. 33 (3), pp.547–567

Balkin (2004) “Virtual Liberty: Freedom to Design and Freedom to Play in Virtual Worlds” *Virginia Law Review*, Vol. 90, pp. 2043-2098

Bargh, J.A. and K.Y.A. McKenna (2004) "The Internet and Social Life" *Annual Revue of Psychology* Volume 55 pp.573-590

Bauman (1997) *Postmodernity and its Discontents* Cambridge: Polity Press

Beck & Beck-Gernsheim (2001) *Individualization: Institutionalized Individualism and its Social and Political Consequences* London: SAGE Publications

Bovaird (2004) “Public–Private Partnerships: from Contested Concepts to Prevalent Practice” *International Review of Administrative Sciences*, Vol 70, pp:199–215

Bruce Schneier, Crypto-Gram Newsletter, October 15, 2000 and October 19th 2007,Web 2.0 Conference in San Fransisco

Castells (1996) *The Information Age: Economy, Society and Culture* Oxford: Blackwell Publishers (3 Volumes)

Castells (2007) “Communication, Power and Counter-Power in the Network Society” *International Journal of Communication* Vol. 1, pp. 238-266

Caudill & Murphy (2000) “Consumer Online Privacy: Legal and Ethical Issues” *Journal of Public policy and Marketing*, Vol. 19 pp.7-19

Cave (2004) "The Cure for the Ills of (e)Democracy is More (e)Democracy: Networked Governance in the Information Society", in: Cunningham & Cunningham (Eds) (2004) *eAdoption and the Knowledge Economy: Issues, Applications, Case Studies*, Amsterdam: IOS Press

Cave (2004) Economic Aspects of Biometrics (draft), http://www2.warwick.ac.uk/fac/soc/economics/staff/faculty/cave/publications/econobiometrics.pdf

Center for Security Studies (2006) *International CIIP Handbook 2006 Vol.1: An Inventory of 20 National and 6 International Critical Information Infrastructure Protection Policies* Zurich: ETH

Center for Security Studies (2006) *International CIIP Handbook 2006 Vol.2* Zurich: ETH

Chellappa & Sin (2005) "Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma" *Information Technology and Management* Vol.6, pp.181–202

Chrystal (2002) *English as a Global Language* Cambridge:: Cambridge University Press

Chrystal (2006) *Language and the Internet* Cambridge: Cambridge University Press

Cogburn, Mueller, McKnight, Klein, & Mathiason, (2005) "The U.S. role in global Internet governance" *Communications Magazine*, IEEE Vol.: 43, Issue: 12

Coleman (2005) "Blogs and the New Politics of Listening" *The Political Quarterly*, Vol. 76:2, pp.272–280

Communication from the Commission to the European Parliament, the Council, The European Economic and social Committee and the committee of the Regions (2007) i2010 - Annual Information Society Report 2007

Crawford & Rutter (2006) "Playing the Game: Performance in Digital Game Audiences", in: Gray, Sandvoss & Harrington (eds) *Fandom: Identities and Communities in a Mediated World* New York: New York University Press

Davis & Silver (2004) "Civil Liberties vs. Security: Public Opinion in the Context of the Terrorist Attacks on America" *American Journal of Political Science* Vol.48 (1), pp. 28–46

Doane Beyond (2005) "Corporate Social Responsibility: minnows, mammoths and markets" *Futures* Vol. 37, pp.215–229

Dutton (2006) "Addressing the Issues of Internet Governance for Development: A Framework for Setting an Agenda for Effective Coordination", Oxford: Oxford Internet Institute, University of Oxford, http://www.intgovforum.org/Substantive_1st_IGF/Dutton-IG4D-30July06.pdf

Dutton and Peltu (2005) *The Emerging Internet Governance Mosaic: Connecting the Pieces*, OII Forum Discussion Paper, No. 5, Oxford: Oxford Internet Institute, University of Oxford

EC Safer Internet Programme: http://ec.europa.eu/saferInternet

Ecotec (2006) "Customer-centric, citizen centric. Should Government learn directly from business?" Prepared DG INFSO, European Commission, http://www.ccegov.eu/downloads/Paper_2_Should_government_learn_from_business.pdf

Ecotec (2006) "Customer-centric, citizen centric. Should Government learn directly from business?" Prepared DG INFSO, European Commission, http://www.ccegov.eu/downloads/Paper_2_Should_government_learn_from_business.pdf; Ecotec (2006) "eGovernment strategy across Europe - a bricolage responding to societal challenges" Prepared DG INFSO, European Commission, http://www.ccegov.eu/downloads/Paper_2_Should_government_learn_from_business.pdf

Ecotec (2006) "eGovernment strategy across Europe - a bricolage responding to societal challenges" Prepared DG INFSO, European Commission, http://www.ccegov.eu/downloads/Paper_2_Should_government_learn_from_business.pdf

ENISA (2007) Information security awareness initiatives: Current practice and the measurement of success, http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_measuring_awareness.pdf

EurActiv.com (2007) "No regulatory holiday in sight for EU telecoms sector" , http://www.euractiv.com/en/infosociety/regulatory-holiday-sight-eu-telecoms-sector/article-165544

European Commission (2007) "Radio Frequency Identification (RFID) in Europe: steps towards a policy framework" http://ec.europa.eu/information_society/policy/rfid/doc/rfid_en.pdf

European Commission Information Society and Media (2005) Information Society Benchmarking Report

Evans & Reddy (2003) "Government Preferences for Promoting open-Source Software: A Solution in Search of a Problem" *Michigan Telecommunications and Technology Law Review* Vol. 19 pp. 313

Felten (2006) 'Nuts and Bolts of Net Neutrality', 11 July, at http://itpolicy.princeton.edu/pub/neutrality.pdf; from RAND, TVWF /AVMS(2006)

Galperin (2005) "Wireless Networks and Rural Development: Opportunities for Latin America" *Information Technologies and International Development* Vol.2 pp: 47–56

Garcia & Horowitz (2006) "The potential for underinvestment in Internet security: implications for regulatory policy" *Journal of Regulatory Economics* Vol. 31 pp:37-55

Gavish & Tucci (2006) "Fraudulent auctions on the Internet" *Electron Commerce Res* Vol. 6, pp. 127–140

Greenstein & Stango (eds.) (2007) *Standards and Public Policy* Cambridge: Cambridge University Press

Hahn & Wallsten (2006) *The Economics of Net Neutrality* Washington, DC: AEI Brookings Joint Center for Regulatory Studies, April 2006

Hahn (eds.) (2003) *Government Policy Toward Open Source Software* Washington D.C.: Brookings Institution Press

G. Heal and H. Kunreuther (2002) " You Only Die Once: Managing Discrete Interdependent Risks" at: http://www2.gsb.columbia.edu/faculty/gheal/EconomicTheoryPapers/discrete.pdf.

Hinde (2002) "Spam, scams, chains, hoaxes and other junk mail" *Computers and Security*, pp. 592-606

Hladjk (2005) "Effective EU and US approaches to spam? – Moves towards a co-ordinated technical and legal response" *Communications Law*, Vol. 10, pp.111-120

House of Lords, Science and Technology Committee (2007) *Personal Internet Security*, Published by the Authority of the House of Lords, http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/165i.pdf

Kampen & Snijkers (2003) "E-Democracy: A Critical Evaluation of the Ultimate E-Dream" *Social Science Computer Review* Vol. 21 pp.491

Katz & Shapiro (1998) "Antitrust in Software Markets" , Prepared for presentation at the Progress and Freedom Foundation conference, Competition, Convergence and the Microsoft Monopoly, February 5, 1998

Kima, Song, Braynov, Rao (2005) "A multidimensional trust formation model in B-to-C e-commerce: a conceptual framework and content analyses of academia/ practitioner perspectives" *Decision Support Systems*, Vol. 40, pp.143-165

Kulathuramaiyer & Balke (2006) "Restricting the View and Connecting the Dots – Dangers of a Web Search Engine Monopoly" *Journal of Universal Computer Science*, vol. 12, pp. 1731-1740

Kumar & Mowshowitz (2006) "Who Should Govern the Internet?" *Communications of the ACM*, Vol. 49, No. 2

Lastowka & Hunter (2004) "The Laws of the Virtual Worlds", *California Law Review*

London Economics in association with PricewaterhouseCoopers (2006) *An Assessment of the Regulatory Framework for Electronic Communications – Growth and Investment in the EU* e-Communications Sector Study for the DG Information Society and Media of the European Commission

Lupia & Matsusaka (2004) "Direct Democracy: New Approaches to Old Questions" *Annual Review of Political Science* Vol. 7 pp.463-482

Malhotra, Kim & Agarwal (2004) "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model" *Information Systems Research* Vol. 15, No. 4, pp. 336-355

Malone (2004) *The Future of Work: How the New Order of Business Will Shape Your Organization, Your Management Style, and Your Life* Boston: Harvard Business School Press

Marsden, C. Cave, J. and Simmons, S. (2008) "Options for and Effectiveness of Internet Self- and Co-Regulation" Report for European Commission, DG INFSO.

Morris (2000) "Contagion", *The Review of Economic Studies*, Vol.67, pp.57-78

Mueller (2002) *Ruling the Root: Internet Governance and the Taming of Cyberspace*, Cambridge, MA: The MIT Press

Newman & Bach (2004) "Self-Regulatory Trajectories in the Shadow of Public Power: Resolving Digital Dilemmas in Europe and the United States" *Governance*, Vol. 17, pp. 387–413

Norris (2003) "Will New Technology Boost Turnout? Evaluating Experiments in E-Voting v. All-Postal Voting Facilities in UK Local Elections" John F. Kennedy School of Government, Harvard University, Faculty Research Working Papers Series

OECD (1998) "Implementing the OECD "Privacy Guidelines" *Electronic Environment Focus on the Internet* http://www.oecd.org/dataoecd/33/43/2096272.pdf

OECD (2001) *Citizens as Partners*, http://213.253.134.43/oecd/pdfs/browseit/4201131E.PDF

OECD (2003) *The e-Government Imperative* http://213.253.134.43/oecd/pdfs/browseit/4203071E.PDF

OECD(2004) *The Development of Broadband Access in Rural and Remote Areas* http://www.oecd.org/dataoecd/29/50/37629410.pdf

OECD (2006) *The Implications of WiMAX for Competition and Regulation* http://www.oecd.org/dataoecd/32/7/36218739.pdf

OECD (2007) *Participative Web and User-created Content: WEB 2.0, WIKIS And Social Networking*, Paris: OECD

Pommerening (2006) "*National Sovereignty and Global Institutions* ", *CIPP Working Paper*, George Mason University

Putnam (1993). *Making Democracy Work: Civic Traditions in Modern Italy* Princeton: Princeton University Press

Sennett (2006) *The Culture of the New Capitalism* New Haven: Yale University Press

Sztompka. (1999) *Trust: A Sociological Theory* Cambridge, CUP

Tapscott, D. and A. Williams (2006) *Wikinomics : How Mass Collaboration Changes Everything* New York: Penguin Group

UK Better Regulation Task Force (2006) *The Principles of Good Regulation*, at: http://www.brc.gov.uk/upload/assets/www.brc.gov.uk/principlesleaflet.pdf

UNESCO (2005) *Measuring Linguistic Diversity on the Internet* Paris: UNESCO

H. Varian (2004) "System Reliability and Free Riding" Advances in Information Security vol. 12:1-15

West (2004) "E-Government and the Transformation of Service Delivery and Citizen Attitudes" *Public Administration Review* Vol. 64 (1), pp.15–27

Wikipedia (2007) http://en.wikipedia.org/wiki/Www#History retrieved on 21.12.2007

Working Group on Internet Governance (2005) *Report of the Working Group on Internet Governance* http://www.wgig.org/docs/WGIGREPORT.pdf

World Bank Institute (2007) *Beyond Public Scrutiny: Stocktaking of Social Accountability in OECD Countries*, http://www.oecd.org/dataoecd/43/3/38983242.pdf

Wu (2003) "Network Neutrality, Broadband Discrimination" *Journal of Telecommunications and High Technology Law* Vol.2 pp.141-180

Zhang & Wolff (2004) "Using Wi-Fi for cost-effective broadband wireless access in rural and remote areas" *Wireless Communications and Networking Conference*, Vol. 3, pp. 1347- 1352

Zixiang (2002) "Testing Theory of Bandwagon – Global Standardization Competition in Mobile Communications", *International Journal of Information Technology & Decision Making*, Vol 1, No 4, p. 615

Appendix C: Methodology

The project started with a horizon scan of literature and RAND's own work in studying the impacts of the ICT related change, and more in particular the aspects relating to ubiquitous connectivity, pervasive computing and emerging socio-economic change. The four themes defined as leading topics for the OECD Ministerial Conference were taken as a guiding structure for the horizon scan: i.e. Infrastructure, Socio-Economic Effects, Reliable Use and Common Trust, Internet governance. For every one of the themes a number of policy topics were identified and described.

The ordered list of topics was reviewed and adjusted in an internal workshop and then sent out to a list of 40 experts to comment on the topics, to suggest additions and to score their relevance. The feedback was processed and sent to the experts again, with information on the first round scores, to achieve a level of convergence around the key issues to address.

These issues were presented in four back-to-back workshops with international experts; dedicating a half a day on every thematic area. The topics were presented by the RAND team, before inviting the experts to discuss. Then the participants were asked to take a perspective of citizen, business or government, to avoid entrenched opinions to be expressed. First a general discussion on the theme helped identify the underlying dilemmas and values, followed by a more in depth discussion on the specific policy challenges and possible approaches.

Overall outcomes of the expert consultation resulted in a clear prioritization of topics:

- Security, reliability, privacy, and trust;
- Self regulation, international and multi-stakeholder governance;
- Net neutrality, and openness of the network.

Also deemed relevant but raising fewer concerns were:

- Social networking and new collaborate approaches
- Return on infrastructure investment; and the relationship between competition policy and innovation;
- Need and effects of global connectivity and access.

There are a number of reasons for this focus. Firstly, there is a focus on security issues as the Internet was not designed for its current use. Secondly, security problems are concrete and there is intense interest around the globe to deal with these issues, which requires action and co-operation across national borders and jurisdictions. Tangible technological and market solutions are available. The high priority given to these issues, as well as the

need to co-operate on a global level in order to be able to make effective improvements, make it a key subject for the OECD conference. Thirdly, the priority issues are all preconditions to achieving the desirable socio-economic outcomes and as such have to be dealt with to enable further development. Finally, these are issues in their own right but have a cross-cutting horizontal nature, which means that they are – in different ways and intensities –relevant across all 4 of the OECD thematic areas. While there may well be a bias in the selected group of experts on the underlying technologies and structures, we feel that these issues do reflect the top priority issues for action at international level.

In two rounds of consultations it became apparent that several issues sparked disagreement among the experts – indicated by strong variance in scoring - with regard to their relevance, or priority for policymaking. As such we believe that these provide an indication towards possible underlying dilemmas. These issues included:

- Level of control, or attempts to such by government
- Relation of private and public sector responsibility
- Relation between the real and virtual world and how to deal with both, as one flows into the other
- Privacy: relevance, universality and changing nature
- Role of monopolies; public subsidy and competition policy
- Security versus uncertainty
- Avoiding, managing, and/or accepting risks
- Identity versus anonymity

The four leading themes set by the OECD, were discussed in the first part of each seminar to determine the most essential topics for deeper consideration. These were:

Theme 1: Infrastructure

- Capacity:
    - Accommodating continued growth (bandwidth and infrastructure)
    - ROI, who invests and who benefits
    - Supply and use of IP addresses (effects on the Developing World)
    - Transition scenarios for Internet upgrades
    - Bottlenecks
- Trust in the network
    - Quality of Service
    - Net Neutrality
- Openness, connectivity, and trust
    - Vulnerabilities: Botnets, Spam, etc.
    - Interoperability and standards

Theme 2: Socio-Economic issues

- Effects and responses to social networking
    - Learning social skills; experiencing social effects
    - Creative commons
    - Virtual connection driving real live mobility

- The new economic paradigm
  - Long tail economics
  - Tipping point tendencies
  - New business models and supply chains
  - Shared creation of wealth; mass collaboration / Wikinomics

Theme 3: Internet governance

- Self- and co-regulation
- Multistakeholder approaches
- International Governance

Theme 4: Reliable use and Common trust.

- Awareness
- Privacy
- Security and openness

The topics were further explored in an issues paper which was discussed with the Ministry of Economic Affairs. Following this interaction and feedback the issue paper was converted into this discussion paper, for which some limited additional sources were researched. As the OECD Agenda is in continuous development, the topics of the seminars and subsequently of this report will not be completely aligned. The authors have endeavoured to map the content to the latest version of the OECD Agenda end-December 2007.

Appendix D: List of Experts

List of participants

Seminar 17 October: Infrastructure, economic and social affairs

Name	Affiliation
Michel van Eeten	Delft University of Technology
Olaf Kolkman	NLnet Labs
Dr Natali Helberger	University of Amsterdam Institute of Information Law
Jaap van Till	Stratix Consulting B.V)
Michiel Westerman	Pink Roccade
Roelof Meijer	SIDN
Rudolf van der Berg	LogicaCMG
Professor Jonathan Cave	Warwick University, RAND Europe

Seminar 18 October: Reliable use, common trust and governance

Name	Affiliation
Marco Plas	Cap Gemini and Jericho Project Research Group
Olaf Kolkman	NLnet Labs
Martin Cave	Warwick University
Paul van Binst	Universitee Libre de Bruxelles
Bart Schermer	ECP.nl and RFID-platform
Jens Arnbak	Delft University of Technology
William Drake	Project on the Information Revolution and Global Governance, Graduate Institute of

	International and Development Studies
Jeanette Hoffman,	London School of Economics and Humboldt University
Eric Huizer	NOB
Jeanne Misfud-Bonnici	Groningen University
Jaap van Till	Stratix Consulting B.V.
Jonathan Cave	Warwick University, RAND Europe
Chris Marsden	University of Essex

Informal support group of the Ministry:

Name	Affilation
Erwin Bleumink	Surfnet
Olaf Kolkman	NLnet Labs
Eric Huizer	NOB
Roelof Meijer	SIDN

Received additional contributions from:

Nico Baken	Delft University of Technology
Leo Koolen	European Commission
Mike Nelson	IBM/ISOC
Vint Cerf	Google
Patrik Fältström	Cisco

Contributors of the Ministry of Economic Affairs

- Jan Wester
- Joost van der Vleuten
- Thomas de Haan
- Rudolf van der Berg
- Ronald van der Luit
- Peter Mandersloot
- Paula Westhoven

- Henk Ruijter
- Jasper Kraaijeveld
- Ed Buddenbaum
- Martin Westerhof
- Robin van Es
- Jos Huigen
- Wim Rullens