



EUROPE

THE ARTS
CHILD POLICY
CIVIL JUSTICE
EDUCATION
ENERGY AND ENVIRONMENT
HEALTH AND HEALTH CARE
INTERNATIONAL AFFAIRS
NATIONAL SECURITY
POPULATION AND AGING
PUBLIC SAFETY
SCIENCE AND TECHNOLOGY
SUBSTANCE ABUSE
TERRORISM AND
HOMELAND SECURITY
TRANSPORTATION AND
INFRASTRUCTURE
WORKFORCE AND WORKPLACE

This PDF document was made available from www.rand.org as a public service of the RAND Corporation.

[Jump down to document](#) ▼

The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world.

Support RAND

[Browse Books & Publications](#)

[Make a charitable contribution](#)

For More Information

Visit RAND at www.rand.org

Explore [RAND Europe](#)

View [document details](#)

Limited Electronic Distribution Rights

This document and trademark(s) contained herein are protected by law as indicated in a notice appearing later in this work. This electronic representation of RAND intellectual property is provided for non-commercial use only. Permission is required from RAND to reproduce, or reuse in another form, any of our research documents for commercial use.

This product is part of the RAND Corporation technical report series. Reports may include research findings on a specific topic that is limited in scope; present discussions of the methodology employed in research; provide literature reviews, survey instruments, modeling exercises, guidelines for practitioners and research professionals, and supporting documentation; or deliver preliminary findings. All RAND reports undergo rigorous peer review to ensure that they meet high standards for research quality and objectivity.

TECHNICAL
R E P O R T

Responsibility in the Global Information Society

Towards Multi-stakeholder Governance

Jonathan Cave, Chris Marsden, Lisa Klautzer,
Ruth Levitt, Constantijn van Oranje-Nassau,
Lila Rabinovich, Neil Robinson

Prepared for British Telecommunications

The research described in this report was prepared for British Telecommunications plc.

British Telecommunications plc
Registered office: 81, Newgate Street, London EC1A 7AJ
www.bt.com

Copyright © 2007 by British Telecommunications plc. All rights reserved.

Preface

BT's annual Hot Topics address controversial issues surrounding the social, environmental and economic impacts of the ICT sector in general, and BT in particular. Their purpose is to assess these issues in a sound and creative way, and foster debate among experts and laymen, government and business, users and service providers. BT's external corporate social responsibility advisory body, the Leadership Panel, plays an active role in the development of each Hot Topic.

For this year's Hot Topic, instead of taking a single issue such as carbon emissions or privacy, BT's Leadership Panel raised an overarching theme: the responsibilities of globally operating ICT companies now that information and telecommunication technologies have become ubiquitous, and central to everyday political, social and economic life.

BT asked RAND Europe to write this year's Hot Topic, contributing RAND Europe's own expertise, investigating and analysing the most relevant literature and views on this subject from selected external experts, as well as from a number of specialists within BT, to shape the debate.

RAND Europe is grateful to all those individuals who offered their expert insights and enabled us to shape the concept of this Hot Topic. The interviewees are listed in the Appendix.

Many issues were raised with us that might merit their own Hot Topic paper. After exploring broad questions concerning the responsibilities of globally operating ICT companies and the ICT sector as a whole, RAND Europe proposed, and BT agreed, that the concept 'multi-stakeholder governance' provides an important basis for contextualising the debate. We intend to open up the debate rather than provide a final word on this subject. We hope to help further critical thinking about how multi-stakeholder governance can responsibly shape the Global Information Society.

For more information about RAND Europe, BT or this document please contact:

Dr. Ruth Levitt
RAND Europe
Westbrook Centre
Milton Road
Cambridge CB4 1YG
Tel: +44 1223 353 329
Email: levitt@rand.org

Susan Morgan
Sustainability Manager,
BT Group plc
BT Centre, 81 Newgate Street
London EC1A 7AJ
Tel: +44 20 7356 4268
Email: susan.2.morgan@bt.com

Contents

Preface	iii
Summary	vii
CHAPTER 1 Global ICT companies and multi-stakeholder responsibility	1
1.1 BT as a global ICT company	1
1.2 ICT companies and the responsibility ‘portfolio’	2
Sharing responsibilities	3
1.3 Multi-stakeholder governance	4
1.4 Sustainability	6
1.5 Challenges and opportunities in the next decade.....	6
1.6 Conclusion	8
CHAPTER 2 The transformative role of ICT	9
2.1 ICT companies and interconnectedness	9
2.1.1 Restructuring and social developments.....	10
2.2 ICT companies and network provision	11
2.2.1 Broadband deployment and NGNs	11
2.2.2 Broadband deployment and the ‘digital divide’	12
2.2.3 Perceptions of resilience and security threats	13
2.2.4 Resilience.....	14
2.2.5 Security.....	15
2.3 ICT companies’ role as information intermediaries.....	18
2.3.1 Responsibility for regulation	18
2.3.2 ‘Web 2.0’	19
2.3.3 Privacy and identity	21
2.3.4 Copyright	25
2.4 Conclusion: Networking raises global governance issues	26
CHAPTER 3 ICT companies and the wider policy environment.....	29
3.1 Wider impacts of ICTs	29
3.1.1 The importance of layered responsibility.....	29
3.1.2 Adjusting global governance to complexity	30
3.2 Approaches to social change: drivers	31
3.2.1 Incentives.....	31

3.2.2	Selection or participation.....	31
3.3	Approaches to social change: recommended actions.....	32
3.3.1	Action 1: Structural rebalancing of roles and responsibilities.....	32
3.3.2	Action 2: Raising the profile of cross-cutting issues.....	33
3.3.3	Action 3: Specific for sector policies.....	35
3.4	Conclusion: Leading the responsibility agenda	37
CHAPTER 4	Specific opportunity areas for BT	39
4.1	Options for BT in redefining multi-stakeholder governance	39
4.1.1	Realigning responsibilities.....	39
4.1.2	The sustainability challenge	40
4.1.3	BT and regulatory relationships	40
4.2	Conclusion: Some ICT-specific recommendations	41
REFERENCES		43
Reference List		45
APPENDIX.....		49
Appendix: List of interviewees		51

Summary

Globally active ICT companies are central to the Global Information Society. They act as:

- network providers connecting people and institutions;
- enablers of innovation, commerce and socio-economic development;
- information intermediaries.

These roles bring significant responsibilities in areas such as security, privacy and sustainability. This paper analyses:

- the responsibilities of ICT companies – and BT in particular – in the Global Information Society;
- the changes that affect the responsibilities of ICT companies as a result of converging technologies and markets;
- the increasing difficulties of compliance with formal regulation and its enforcement;
- how ICT companies may act responsibly in the future.

However, the Global Information Society is also multi-stakeholder. It is composed of relationships between ICT networks and non-ICT firms, governments, NGOs, consumers etc., each of which participates in a variety of roles; so it is also a multilayered, complex system.

In order to meet the challenges of the above mentioned responsibilities, a new, multilayered, multi-stakeholder dynamic concept of responsibility is necessary. Individual stakeholders and the sector as a whole must engage in effective, collaborative ways, balancing the benefits of inclusiveness and consultation on one side and effectiveness in directing and enforcement on the other. This report suggests three 'actions':

- structured rebalancing;
- cross-cutting awareness;
- sector-specific engagement.

The structural rebalancing of responsibilities is based on:

- who can best bear it;
- the alignment of interests;
- effective leverage.

Such a development can only be effectively achieved if enhanced by awareness-raising around cross-cutting issues, such as:

- security;
- enforcement;
- privacy;
- sustainability.

At the same time, thematic targeted engagement specific to each sector is required on essential policy domains:

- privacy;
- communication rights;
- digital inclusiveness;
- security;
- reliability.

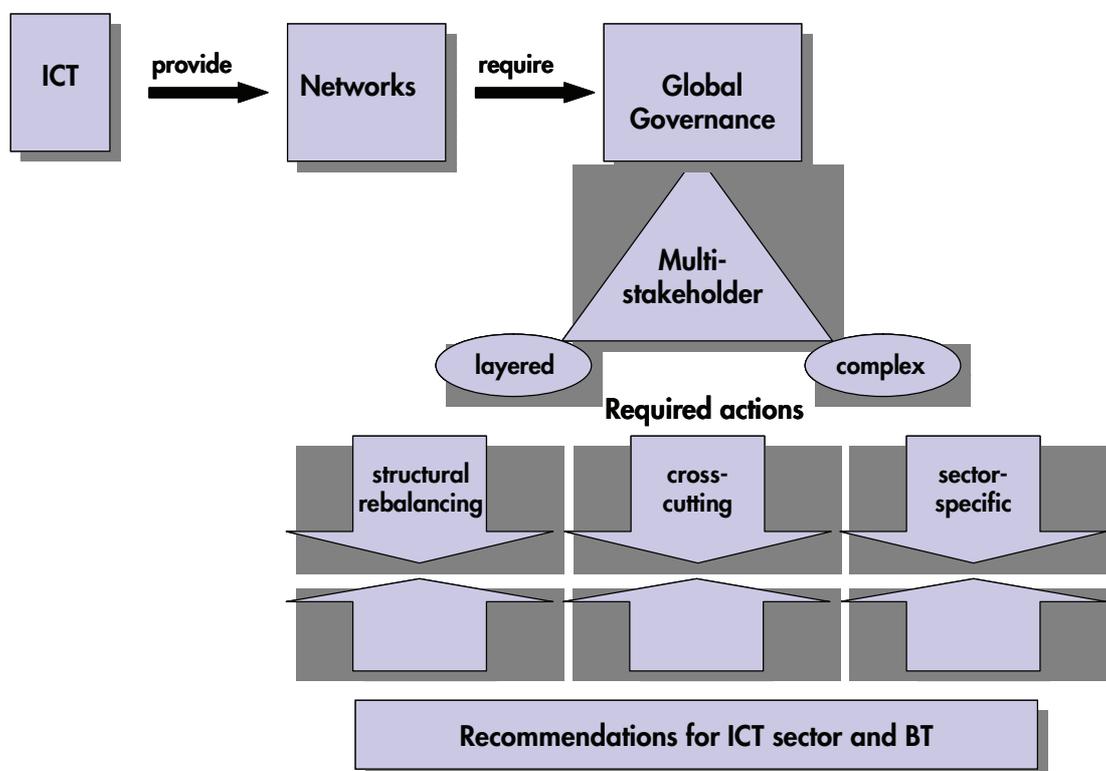


Figure 1 Conceptual logic

BT occupies a relatively unique position due to the UK ICT sector's pre-eminence in addressing many of these problems, and BT's own:

- engagement with these social issues;
- relationships with its regulator;
- roles as the pre-eminent incumbent (telecom network provider) in its home market, and competitor and strategic partner of competitors across the globe.

Its diverse business and legal environment also means that BT's own internal governance has a strong multi-stakeholder quality. BT can thus assume a leadership role in actions to strengthen global governance, by:

- resolving internal coordination issues;
- leveraging strategic power to address problems;
- serving as a Corporate Social Responsibility exemplar and a mobiliser of multi-stakeholder governance;
- finding a platform for pro-active engagement that minimises the inevitable suspicion of 'special pleading'.

This report recommends two specific ways in which BT can further advance its already very active engagement as a global corporate citizen and exemplar:

- further reinforce its sustainability operations down the supply chain in developing countries, by extending its mainly post-contract assessment to the pre-contract phase;
- exercise 'ethical leadership' in promoting further integration of decision-making on commercial and 'responsibility' strategies, and helping all stakeholders to share in progress towards advancing the sustainability agenda.

CHAPTER 1 **Global ICT companies and multi-stakeholder responsibility**

In Chapter 1, we:

- define key issues of *responsibility* for an ICT company operating in an interdependent relationship with other stakeholders;
- lay down the rationale for sharing responsibility;
- outline the need for and complexities of multi-stakeholder governance;
- discuss, briefly, different aspects of sustainability;
- look to future, cultural challenges facing the Global Information Society.

1.1 **BT as a global ICT company**

Corporate social responsibility (CSR) is no longer considered an add-on or as philanthropy, but as an integrated business activity. CSR has a diverse agenda, including:

- sustainability;
- brand management;
- development;
- human rights. (COM 2006; EC Green Paper 2001; European Multi-stakeholder Forum Review 2006)

As the Information and Communication Technology (ICT) industry has a key enabling role in social, economic and human development, the deployment of these technologies, and the changes in behaviour and governance that result, both magnify collective problems

Global operation means a wider range of unpredictable impacts and reputation risks. To manage this it is important that companies are linked up in the right networks involving their competitors, stakeholders, NGO's and others in order to know what is going on and to anticipate what the future is likely to bring.

Mark Goyder
Founder Director, Tomorrow's Company,
and member of BT's Leadership Panel

and create the infrastructure for effective collective action to address them.

As a global ICT company, BT has responsibilities in the international political economy, in addition to its well-defined national role. Competing with other pre-eminent telecommunications companies and incumbents across the world as a business service provider, it also has a responsibility to influence agendas through example or coalition-building rather than using its market power to act independently. Thus it has a dual role as:

- global corporate citizen; and
- competitive player.

Abroad, however, it is more interdependent on its suppliers, customers and host governments than in its UK 'home' market.

1.2 ICT companies and the responsibility 'portfolio'

ICTs are societal technologies; that is, they inform and connect people, and change their engagement with each other, their economic environment and their relationships with government. This imposes a certain 'portfolio' of responsibilities on key ICT companies. However, it is important to distinguish between the responsibilities and how they are best discharged, in particular, differentiating between collective and individual responsibilities and roles. The challenge is simultaneously to deal with current responsibilities and expectations while moving to a 'better' allocation of responsibility. In achieving a reallocation of responsibility and in taking action to address societal problems, the individual and collective levels are interdependent. For instance, the effectiveness of multi-stakeholder activity depends on contributions by individual entities. Conversely, individual action can pre-empt collective willingness to address mutual issues.

There are three important levels of activity companies have to perform for being leaders regarding their responsibility: First, govern themselves effectively. Secondly, join others (other companies, civil society groups, international agencies) to work on issues they cannot solve alone. Thirdly, lobby governments to put the right regulations in place even though this might mean some profit losses in the short term.

Issues facing ICT companies regarding responsibility are:

Christopher Marsden
Chair of Amnesty's Business Group

- *minimisation or responsibility avoidance*, that is, whether a company acts proactively to:
 - reduce the risks from which responsibilities flow;
 - minimise associated harms;
 - encourage and help those affected to look out for themselves;or
 - fails to discharge their proper responsibilities;
 - accedes to (arguably) inappropriate requests from host governments;

- *diversification of responsibilities*, that is, which aspects of responsibility are particular to the home market, with its longstanding regulatory relationships and obligations, and which can be transferred to other markets and operating environments;
- *transfer or acceptance of responsibility*, that is, whether ICT firms best placed to manage responsibilities choose to embrace or accept them, e.g. proactive steps by Internet Service Providers (ISPs) acting as information intermediaries. The degree of acceptance of responsibility may reflect the size and competitive position of a company and thus differ between home and host markets.

BT is a notably 'unified' regulatory actor, taking a similar view of competition and market entry in home and host markets, as illustrated by its membership of the European Competitive Telecoms Association (ECTA). Its responsibility strategy may thus learn from its regulatory strategy. Beyond this, the portfolio of responsibilities may become more manageable through a combination of:

- critical mass – enhancing leadership and leverage;
- internalising cross-effects – e.g. between the economic and environmental aspects of sustainability;
- development of cross-cutting or joint strategies and diversification – offsetting developments in one domain by developments in another.

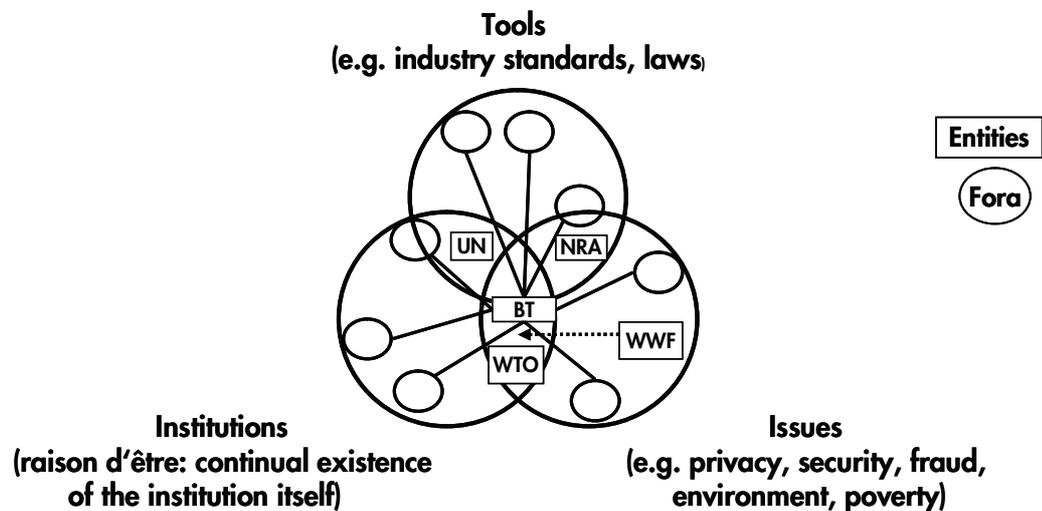


Figure 2. Conceptualisation of Multi-stakeholder approach

Sharing responsibilities

Companies can place responsibilities on a 'joint and several' footing with an appropriate alignment of powers, motives and information via:

- co-regulation – where they regulate activities in partnership with government;
- or
- self-regulatory institutions – where companies choose to regulate themselves.

For example, various ISP associations across Europe and elsewhere have used the model of the Internet Watch Foundation to help police illegal content on the Internet. Such institutions properly need to consider the rights and responsibilities of those who may be affected by their activities, for instance, customers, government and civil society, and such

One of the key future trends is a much stronger link between the CSR agenda and public policy agenda.

Jane Nelson

Director of Corporate Social Responsibility Initiative
at the JFK School of Governance

responsibility is not cost-free. Firms seeking to change their responsibility portfolios may need to secure investor commitment. Smaller and less established companies may also 'free ride' on the good corporate citizenship of others.

However, sharing responsibilities is the first step towards multi-stakeholder governance.

1.3 Multi-stakeholder governance

The inability of national governments to regulate much of the Global Information Society increases the importance of cooperation in finding solutions. More legitimate and inclusive corporate involvement is desired than simply classic ICT industry self-regulation through, for instance, standard setting. This novel approach to corporate involvement is described as 'multi-stakeholder governance'.

Any joint issue can be addressed by a combination of:

- individual self-interested action;
- regulatory 'rule-setting';
- deliberative consideration and coordination.

However, if these arrangements become institutionalised, they can lead to inflexibility and exclusiveness. In response to new problems and opportunities, this static picture of controlled rational behaviour is changing in the following ways:

- co- and self-regulatory institutions are developing to deal with both new and old issues;
- linkages, such as economic approaches to technical or societal problems, are increasingly open to scrutiny.

One consequence of this is a *layered view of governance* in which key stakeholders combine collective action to address mutual issues with changes in their own commercial, or other, behaviour.

One of the important things of corporate responsibility is debate and discussion, openness and accountability.

Dunstan Hope

Director at Business for Social Responsibility (BSR)

This *active citizenship*, which emerges clearly from the evidence and insights presented in the following chapters, integrates public and private responsibility. A multi-stakeholder approach may not be an optional extra but essential to address

pressing and cross-linked issues coherently and legitimately.

Debates around responsibility and the Internet exemplify experimentation with the roles of companies, governments and consumers/citizens (Lessig 1998) and provide an influential framework for examining the future of governance and responsibility. The term 'governance' is used to differentiate power relations from the 'hard' rules of government.¹ 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. (Hoffman 2005)

This equally applies to the responsibilities of global ICT firms such as BT in expanding from a national telecoms company into a less defined global role (MacLean 2004, 73–99; Mueller et al. 2004). Internet governance is not simply inter-governmental, technical or market-led, but also, critically, involves Internet *users* (Kummer 2004, 53–57). This is exemplified in the United Nations Working Group on Internet Governance (WGIG; UN Report 2005) and its successor, Internet Governance Forum.²

Learning from the others is key; in terms of collective action by groups of companies, the extractive, food and pharmaceutical industries have been more effective than the ICT sector in tackling difficult issues, although some interesting collective initiatives within the ICT sector are starting to emerge.

Jane Nelson
Director of Corporate Social Responsibility Initiative
at the JFK School of Governance

The idea that roles and responsibilities in the global and highly dynamic environment enabled by ICT can be allocated on a temporary and contingent basis, according to inclusive and non-hierarchical relationships, is of course not new. Roles have often shifted among government, corporations and civil society (consider the Red Cross or the British East India Company's histories) but it appears that the United Nations is underwriting a more durable, multi-stakeholder relationship in regard to Internet governance. This is a novel and fascinating attempt to achieve real global dialogue around responsibilities in the Global Information Society, and may be a significant new governance paradigm.

¹ See Kooiman (2003) p. 23: 'Anyone involved in governing, in whatever capacity or authority, forms images about what he or she is governing.... Even implicit images govern those who govern. Governing images are always there; however, they can certainly be (re)created and changed. During image formation, governing challenges will be defined and formulated as governing issues'. See also Kleinwächter (2004).

² See the Internet Governance Forum (IGF) at: <http://www.intgovforum.org/>. Other such international co- and self-regulation experiments are: CONGO (the Conference of Non-Governmental Organisations), ICANN (the Internet Corporation for Assigning Names and Numbers), and locally through, for example, the UK telecommunications regulator Ofcom, which is conducting a long-term study of such arrangements in 2007.

1.4 Sustainability

Multi-stakeholder governance arises most naturally in relation to common problems of corporate responsibility, specifically where outcomes depend on engagement at different levels (individual, sectoral, national, etc.). Sustainability is an obvious example of such a problem.

For many, sustainability equals environmental sustainability. The ICT sector has good reasons to be involved with this important aspect as large ICT companies are directly responsible for the emission of large volumes of greenhouse gases and indirectly responsible for their customers' even greater emissions; while the effects of ICTs on environmental sustainability in the wider economy (e.g. on transport) are even more profound.

It may also be argued that ICT companies have a moral obligation to engage with sustainability due to their profoundly transforming role, relatively large economic surpluses and substantial associated environmental rebounds.

The Brundtland Commission defined sustainable development as,

development that meets the needs of the present without compromising the ability of future generations to meet their own needs.

It thus considered economic, socio-political and environmental dimensions. (Brundtland Commission 1987) Recently, this has been expanded to include cultural sustainability.³ These domains are not independent: for instance, political or economic mechanisms can exacerbate or help resolve problems in other domains and they cannot be considered in isolation.

In essence, sustainability embodies some concepts of 'security' in the broadest sense of the word. Insights into issues such as security, privacy, fraud, raised by interviewees (see Appendix) may be considered as part of the broader sustainability debate, especially economic and socio-political sustainability, while specific policy topics, such as ownership and informed consent, apply equally to cultural and environmental sustainability as to specific ICT policies.

The interconnected nature of the Global Information Society exacerbates the need to deal with these issues in a holistic multi-stakeholder approach. It also provides scope for the dual strategy of leadership and exemplary action that we use to define global citizenship within this framework.

1.5 Challenges and opportunities in the next decade

We consider current challenges and benefits in the remainder of this paper and attempt to think ahead to 2017 to consider the significance of the continued transformation of the ICT industry, and through that, the wider political economy.

One further challenge is cultural: the ICT sector is often perceived as an outgrowth of a (somewhat synthetic) amalgam of 'Western' economic, business, social and political

³ See e.g. the documents produced by the EC-funded TERRA2000 project at: www.terra-2000.org

attitudes and values. The reality has shifted with the globalisation both of the sector and of the values, and with profound changes in the economic and political order throughout the world.⁴ However, the impression persists and is even amplified by the intimate association of ICTs and Western governments and people. This provides both challenges and opportunities. As one of the most visible interfaces between the developed, emergent and developing 'worlds', ICTs are often cited as strategic instruments of hegemony and imposed change, or as strategic targets for attacks ranging from rhetoric to terrorism. But this prominence, and the very active role taken by some ICT firms in unbundling the tools of societal transformation from the objectives of developed Western economies, allow the sector to drive the debate beyond a simplistic 'clash of civilisations' dualism. This can be summed up in a few simple challenges:

The biggest challenge is that the rules are national, but the Knowledge Society is global.

Markus Kummer

Executive Coordinator of the IGF Secretariat

- How can ICT companies best engage with government, business and civil society in pursuit of their own goals?
- How can ICT companies play effective and positive public roles in facilitating closer links and great communication *within* government, business and civil society?
- How can ICT companies act to reduce the distances *between* peoples, governments, companies and consumers?

The first provides a basis for deciding in an open, transparent and effective manner, how and under what circumstances to take account of the uses to which ICT services are put, and the further consequences of those uses. It involves engagement with:

- 'better regulation' goals of open and fairly competitive markets;
- transparent governance and limited state intervention;
- pro-active support for policy in relation to 'public goods' (health, education, etc.) and 'public bads' (crime, conflict, poverty, etc.).

What you have got is essentially an ungoverned or under-governed global economy, in which clearly corporations have to take a much larger role in governance if we want to have a world that is going to work.

Christopher Marsden

Chair of Amnesty's Business Group

The second and third challenges are based on the critical impact of communication on governance within and among the public, business and civil society spheres, and the importance of mediating an appropriate balance between coordination on one side and independence and competition on the other.

⁴ The ICT sector increasingly involves powerful players arising in the emergent economies of China, India, Brazil etc. The dominant business culture is more global than American and connection between various conceptions of market capitalism and democracy are realigning throughout the world.

1.6 Conclusion

This chapter has focussed on the key transformative question: how can a globally responsible ICT company, such as BT, address the political economy 'governance gap?'

When ICT companies operating inside national markets and under national regulations create new multinational markets, they also create new issues regarding their responsibilities to others in the broader environment, and the extent to which they should act as a neutral agent or change their own conduct. Companies will need to address such issues by, for instance:

- making decisions on interoperable standards;
- using new techniques to identify customers and citizens in networks using open protocols;
- developing technologies to prevent harmful content reaching end-users;
- changes in wealth creation and job security.

They will also need to look at insourcing and off-shoring and ramifications to the wider environment. Above all, they will need to move towards a layered view of governance, with key stakeholders combining to take collective action to address mutual issues. The rest of this report illustrates multi-stakeholder themes for global ICT companies by role and responsibility.

In this chapter, we first present a ‘thumbnail’ portrait of the turbulent past and present of the ICT sector and its effect on economies and societies. Next, we examine ICT companies’ challenges and responsibilities as providers of network connectivity, and then as information intermediaries.

2.1 **ICT companies and interconnectedness**

The world is now more connected, with greater interdependence than ever before, politically, socially, economically and culturally. This interdependence brings economies of scale for positive developments, for example:

- prices and opportunities favouring connectivity;
- global opportunities make unlimited free phone calls possible to one's family;

and negative developments, for example:

- risks of being used for political or religiously motivated attacks;
- unlimited attacks on other people's property and wealth.

ICTs offer transformative opportunities for both good and bad.(Brown et al 2006)

Using and misusing ICT

- 500 million people have downloaded the Skype Voice over Internet Protocol (VoIP) application software.⁵
- Two billion mobile phones are in some type of use.⁶
- Governments and corporations are extending their abilities to monitor and record human activity and movement.
- Up to 25% (150 million) of the PCs currently connected to the Internet are already part of botnets⁷

⁵ Tech Digest: http://techdigest.tv/2007/03/skype_boasts_50.html#more

⁶ BBC News 11 January 2006: http://news.bbc.co.uk/1/hi/programmes/documentary_archive/4603284.stm

⁷ Vint Cerf's address to the World Economic Forum in Davos, <http://news.bbc.co.uk/1/hi/business/6298641.stm>. Botnets are collections of compromised computers that run autonomously;

2.1.1 Restructuring and social developments

Some ICT companies were guilty of exaggerating the pace of change in the global economy brought on by ICTs, and therefore the expected growth of the ICT industry itself, increasing the largely self-inflicted severity of the 2001–3 'dot-com crash.' This led to thorough consolidation of the ICT sector and restructuring of individual companies and sectors most reliant on ICTs, such as financial services and accounting. International banking and insurance took advantage of new connectivity, analytical tools and opportunities for risk management in global trading. Most notably for consumers in broadband-enabled economies, e-commerce enabled real economies and greater choice in budget air travel, the wider holiday business, retail banking and insurance.

In particular, the explosive growth of business and consumer electronic 'auctions', such as eBay, illustrates the connections between societal and commercial networks, and sustainability and opportunism. On the positive side:

- the enormous expansion of resale of material goods reduces waste, thus promoting material sustainability;
- new markets are opened up to consumers who could not have afforded the same goods when new;
- many individuals have become full-time online traders;
- electronic auctions provide a truly national, even global distribution platform for small businesses and start-ups.

On the negative side, such auction sites:

- provide distribution channels for stolen and fraudulent goods;
- may crowd out local resale outlets (classified adverts, boot sales, etc.) generating substantial transportation flows.

Government services and information sharing are also being transformed by ICTs, despite the disappointing early results of significant public investments in technology, to enable e-government, e-education and e-health services.

With over 10 million domestic consumers having subscribed to broadband in the UK, the five years since the dot-com crash have seen a majority of the Northern European, East Asian and North American population accessing the high-speed Internet and therefore creating a mass market for digital ICT products and e-commerce. As this boom begins to generate further demand, many have begun talking about the arrival of Web 2.0 where user-generated content is commonplace and the consumer acts as both beta tester of new ICT products, shaping their evolution, and creating new value from existing user-generated content.

While all these changes have created tremendous potential for dynamic innovation, they have put strain on the static business models of pre-existing industries, as well as governments' ability to regulate.

2.2 ICT companies and network provision

The first responsibility of public communications network providers is to their customers, to provide:

- the connectivity for which they pay;
- security and resilience of the digital infrastructure and its physical assets.

We shall focus on next generation networks (NGNs) and their security and resilience to frame the roles of network providers in broad terms that apply to end-users and public policy debate, in particular:

- social issues arising from market developments;
- the critical importance of individual players and framework conditions;
- the network effects underlying a far broader range of societal issues.

2.2.1 Broadband deployment and NGNs

The need for a fresh approach to ‘human’ (economic and social) issues in technology deployment was emphasised by the US National Science Foundation in terms of quality of service and security.(Clarke 2005; Marcus 2004)

It is widely believed that the transition from traditional circuit-switched telephony towards packet-based NGNs is a substantial efficiency improvement in networking with the potential significantly to transform the business and residential consumer’s experience.(Cave et al 2006, 242–55) The speed and extent of this transformation are matters for regulation, economics, and social policy. However, they also create issues around the reciprocal impact of technical, economic socio-political and environmental responsibilities.

While some networks will carry data at very great speeds, responsibility is likely to focus on the deployment of networks offering more ubiquity of access than speed (see 2.2.2 below).⁸ There is already a very wide range of broadband products that combine characteristics of being ‘always-on’, with sufficient bandwidth to permit high quality files (such as video) to be transferred. An important issue is whether data traffic will separate into different ‘speed lanes’ with crash barriers defined by different applications and ways of accessing data, or will converge on a common infrastructure/service offer. The change to NGNs creates new opportunities for de- and co-regulation as well as new potential for incumbents to invest in access bottlenecks.⁹ Key broadband investment and technology decisions by incumbents and competitors depend on their assessment of various regulatory and other framework factors.¹⁰ Only Japan, for instance, has completed the negotiation of the new Reference Interconnect Offer (RIO) for NGNs (Katagiri 2006).

⁸ Talbot (2006) explains that 400Gbps is the expected throughput of Internet2 in 2007.

⁹ See Marsden (2006). There is very little non-technical academic literature on this subject due to its novelty.

¹⁰ A central issue is whether the future will entail locally owned local connections from the telephone exchange to the subscriber’s premises (e.g. municipal fibre as in Stockholm) that could be shared with multiple providers, so that competition takes place “beyond the last mile”. See e.g. OECD Foresight Forum (2006).

This process is an example of multi-stakeholder governance at work, but its technically forbidding nature makes broader inclusive debate problematic.

2.2.2 Broadband deployment and the 'digital divide'

Broadband deployment depends on:

- the linked socioeconomic inequalities grouped under the term 'digital divide';
- network availability and sustainability;
- the safety of both packets and their content (see 2.2.3–5).

'Universal' access/service is at heart a public good, but there are technical issues around the digital divide relating to inequalities of:

- education;
- age;
- socio-economic status;
- accessibility for the sensory-impaired, etc.

To draw out the implications of these, we shall focus on *threshold connectivity*.

The 'speed' of a broadband connection is by no means the only determinant of effective transmission; connectivity depends on:

- throughput;
- latency (delays or lack of signal continuity);
- reliability.

These in turn depend jointly on:

- network capacity management;
- user-generated congestion.

Services such as streamed media, gaming or telephony depend on more symmetric and synchronous availability. Congestion effects deriving from contention (congestion at local access points) arise from and directly constrain the growth of access and connectivity. File compression, particularly of video, is improving rapidly, with latest generation several times more powerful, leading initially to more efficient use of capacity. However, higher performance and quality draw in more intensive network users, with the potential for rebound effects – the networks becoming victims of their success.

Some deteriorations, such as 'burstiness' or alternation of the connection, that depend on network load are less damaging to asymmetric uses, for instance downloading content for later

What you see in terms of the cell phone use in Africa is a fabulous example of technical leapfrogging. It creates local wealth, local opportunities, and has the potential for positive political impact.

Jane Nelson
Director of Corporate Social Responsibility Initiative
at the JFK School of Governance

access. Networks for distributing files are increasingly efficient – peer-to-peer (P2P) networks take advantage of distributed file sharing, preventing overloading at one point in the network – while at the same time weakening the ‘client-server’ power relationships on which regulatory responsibilities have traditionally been assigned. The realignment and devolution of power may be more efficient in some ways, but raise other issues that multi-stakeholder governance must resolve. The key ambiguity is whether the ‘rules’ amount to an inefficient way for those ‘dispossessed’ by P2P to regain (or extend) power. These observations carry several specific implications.

- Technological fixes for technological problems carry potentially profound societal implications, but are not generally implemented in ways that take these into consideration.
- Individual behaviour will always try to ‘route around’ obstacles, even if the consequence is increased inequality.
- Rerouting and other changes associated with user behavioural and technological responses to NGN Quality of Service issues may move the ‘efficient’ locus of responsibility (where it is best discharged) away from its traditional or even institutionalised home at the ISP and into different responsibilities.

2.2.3 Perceptions of resilience and security threats

As long as systems are open enough and have enough redundancy they should be able to absorb attacks.

John Dryden
OECD Deputy Director, Science, Technology and Industry

Increased dependence on ICT and its integration into all aspects of our lives throws into acute relief the importance of ICT security.¹¹ While organisations and consumers get used to the most recent technological development and devise ways to meet the accompanying challenges, criminals and opportunist stay one step ahead of the game:

- P2P networks are ideal for exploiting illegal content;
- ‘phishing’ takes advantage of necessary trust in electronic communications;¹²
- mobile phones have become attractive targets for street robbery.

There are two main issues to consider:

- resilience and robustness of the communications network to cope with disruption;
- data security.

¹¹ According to Eurostat in the beginning of 2006 around 52% of the households of the 25 European countries, and 94% of enterprises with at least 10 employees had access to the Internet; nearly half of individuals in the EU25 used the internet at least once a week in 2006; a third of households and three-quarters of enterprises had broadband internet access

¹²Phishing is a scam involving sending seemingly legitimate emails which trick victims into submitting sensitive personal or financial data to a fake website which appears to be legitimate.

Note that these risks to hardware, software, services, information and other assets and ICT societal uses in general are connected with:

- complexity *per se*;
- accidents and strategic attack;
- criminal misuse.

Framing them too narrowly may produce policies that are insufficient to protect infrastructure resilience, or the security of communications and content.

Perceptions of security threats

The general public, industry and government have diverse views of security threats. While these overlap to some degree, there are some overall differences.

Consumers' participation and behaviour online are most influenced by concerns about:

- identity theft – the crime of impersonating someone, using their private information, for financial gain (www.getsafeonline.org);
- spam – unsolicited commercial e-mail, also known as junk e-mail;
- denial of service.

Industry has tended to focus more on the problem of sustaining infrastructure integrity in the face of increasing openness in the technical protocols and rapidly rising levels of use.

Public sector concerns, not always embraced, include both principled and pragmatic consequences for trust and confidence from malicious and damaging activities.

Private parties seem relatively insensitive to the consequences of, for example, privacy breaches and phishing. This lack of response and recognition by those closest to the risks can undermine such 'public goods' as the rule of law to international economic competitiveness. Private parties are not taking the actions necessary to minimise the risks at 'ground level' and do not see the risks as justifying the civil liberties consequences of legal action. This in turn can undermine trust in the online economy and thus harm competitiveness.

2.2.4 Resilience

'Protocols' (rules) used to transmit data over the Internet automatically divert around problems or outages, giving the network a unique resilience and ability to withstand random attacks or disruption. However, this property becomes weakened if certain points in the network are selected for attack. Although the Internet is clearly a robust global phenomenon, it retains unique local vulnerabilities of:

- content – software vulnerabilities, security breaches in important organisations;
- physical structure – fibre optic infrastructures, availability of communication links, vulnerability of major elements to man-made or natural disasters.

The repercussions of physical and logical attacks can be life threatening; dangerous, for example, the Distributed Denial of Service (DDoS) attack that forced closure of the port

of Houston; or have financial, time or nuisance costs, as with phishing, identity theft and spam.¹³

Increasing reliance on mobile and Internet infrastructures brings increasing vulnerability to events in the physical world. Computer networks, generally dependent on electricity supplies, are at risk from power failures.

Vulnerability of mobile demand

The London Assembly report into the 7/7 bombings noted that mobile phone communication networks became seriously overloaded as a result of the incident, severely hampering the ability of the emergency services to do their jobs. This vulnerability to mobile demand surge is becoming increasingly common in the wake of natural disasters such as flood, tsunami and earthquake, especially those that knock out fixed-line infrastructures.

Note that these risks arise directly from reliance on alternative and enhanced communications that improve the resilience of societal infrastructures. For example, the impaired function of mobile networks in the wake of natural disasters is testimony to the crucial role of such communications.

As long as systems are open enough and have enough redundancy they should be able to absorb attacks.

John Dryden

OECD Deputy Director, Science, Technology and Industry

Resilience and robustness in infrastructures and ecosystems rely on appropriate redundancy and diversity and not on winner-takes-all dominance by a lean and mean 'best' solution. The multiplicity of stakeholders is clear: even home WiFi¹⁴ users can be part of both:

- problem – unauthorized use of their network by third parties creates security risks; and
- solution – providing an alternative semi-public infrastructure.

2.2.5 Security

Regulation and interoperability, for example, European-level suggestions for network and information security strategies considered or enforced at national level, play critical security roles in broadband provision. However, these impose nontrivial costs over and above existing costs protecting subscribers against spam, DDoS attacks, phishing and other crimes.

¹³ DDoS attacks result when attackers use software codes covertly placed on a victim's machine to then launch an Denial of Service (DoS) attack against a third party website or online information resource, rendering a server unusable by the sheer number of web-page requests made. The attacker's computer, using specialised software, can control hundreds of thousands of 'compromised' computers. See BBC news website October 17 2003 'Questions cloud cyber crime cases'.

¹⁴ "Wireless fidelity" refers to a wireless local area network based on the 802.11 standard.

Businesses are also responsible for keeping data safe and secure. If not managed properly, risks stemming from poor data security practices and global vulnerabilities undermine trust and confidence in the Internet, undoing much good work by national and regional authorities to encourage demand. This problem grows with use, the critical information infrastructure centrality of broadband, and ICT evolution towards pervasive computing and machine-to-machine communication. (ITU Internet Reports 2005 ‘The Internet of Things’) There is an escalating ‘arms race’ as attacking, opportunistic and defensive behaviour become more sophisticated and burdensome. (Brown et al 2006)

- Attacks have evolved from unauthorised access and data theft to data corruption/exposure or access denial.
- Defence has changed data collection/storage/processing centralisation, patterns of data exchange and liability allocation among buyers, sellers and ISPs.¹⁵

This is all part of the evolutionary play being performed by multi-stakeholder parties in the market/regulatory ‘theatre’. They are not a sign that things are necessarily getting worse. The new environment provides greater scope for:

- rapid detection and systemic response to threats;
- awareness-raising;
- communication and coordination against a range of vulnerabilities;
- technological approaches (eg, identity technologies like chip and pin, biometrics) that have already proven their worth in specific applications.

These positive responses mix technological and ‘soft’ strategies at individual and aggregate levels.

The risk is that we end up with a fragmented Internet or an Internet that does not facilitate the free flow of information.

Ayesha Hassan

The resulting changes in network topology include:

Senior Policy Manager for E-Business, IT and Telecoms,
International Chamber of Commerce

- protected ‘walled garden’ environments with users and content kept safe (or safely) behind ISP, corporate or national ‘firewalls’;¹⁶
- Virtual Private Networks.

Potential casualties of security concerns include:

- Internet openness;

¹⁵ One of the key complexities concerns the liabilities arising from data transfer between different data protection regimes.

¹⁶ BBC 6 January 2006: http://news.bbc.co.uk/1/hi/programmes/click_online/4587622.stm; Wikipedia: http://en.wikipedia.org/wiki/Internet_censorship_in_the_People's_Republic_of_China

- end-to-end connectivity;
- privacy – in some ways the mirror of security.

Differences between the developed and developing world are significant in terms of the coherence and pace of technological development. However, these worlds also interact strongly (eg, hackers residing in Ukraine or North Korea, or hijacked computers sending spam from Florida).

This problem is beyond the powers of any one sector or organisation. Public, private and civil society organisations must collaborate. In addition to overlapping interests, they have complementary competences:

- the state has power to regulate many areas of civic and business life;
- business has technical organisational scope to change products, services and processes;
- citizens can take detailed personal or community responsibility, implementing precautions that would be oppressive at national or market level and acting as ‘trip-wires’ or early-warning systems for emerging threats.

For example, the main source of DDoS attacks is unprotected broadband-connected home computers.(BCS ‘Managing the Risks’ 1507) Effective response requires:

- consumer responsibility – keeping computers protected and security software up to date;
- industry action – e.g. ISP technical and informational means of identifying patterns and mitigating harms;
- government action – strengthening enforcement and criminalising such activities.

Information security standards also help to underpin security. International bodies can also encourage shared approaches and solutions that markets cannot or will not provide unaided.¹⁷

ICT companies provide security for others via network deployment and management, for example, the UK’s NHS data spine. This has led to the emergence of stand-alone and bundled

The problem is that law enforcement agencies do not have the necessary skills and expertise to know exactly what information they require to track terrorist on the Internet. They don't know what information to ask for and usually ask for everything. They have a lot of learning to do and Industry can contribute to this learning and help combat terrorism.

Tom Mullen
Head of Security Investigation Services, BT

¹⁷ These include the International Chamber of Commerce, Organisation for Economic Co-operation and Development (OECD), European Union, Council of Europe and G8. The World Summit on the Information Society, as well as its forerunner Dotforce (Digital Opportunities Taskforce 2001) and the Global Alliance for ICT and Development have also engaged multi-stakeholder discussion and action around these vital issues.

security-enhancing goods and services and even markets for identity and security. ICT companies also provide crucial exemplars and practical application for public and private sector clients, as with the UK government-industry Get Safe Online partnership.(<http://www.getsafeonline.org/>) Such partnerships are crucial for government and industry; each has information and competences needed to identify and effectively address continuously changing threats.

2.3 ICT companies' role as information intermediaries

ICT companies not only provide connectivity, they filter information provided by content providers to end-users and among producers and consumers, including the important new category of Web2.0 user-producer-editors. We consider the issues this raises of responsibility for regulation, and then the implications of Web2.0 in relation to specific topics of:

- privacy
- copyright.

The discussion shows that the changing relations unleashed by the development of the sector inevitably place ICT firms in the centre of societal governance.

2.3.1 Responsibility for regulation

Initially, this filtration was seen as enforcement of 'real-world' rules and regulations via 'virtual' mechanisms. Key Internet players potentially have particular advantages in detecting and sanctioning 'undesirable' content and communications. As centrality of Internet-enabled communications becomes critical, these responsibilities become indispensable to conventional regulation and law enforcement. However, ICT firms lack the standing and accountability to establish, enforce or interpret laws in even a single jurisdiction, let alone to mediate international differences. Yet they face pressure from governments, citizens and other businesses to discharge or avoid these responsibilities in particular ways.

The interconnected nature of the Internet ensures that individual firms' actions can generally be circumvented; best effort and weakest-link actions must therefore be considered jointly among stakeholders to:

- identify key issues;
- develop a coherent and consistent response.

The objective is neither a single set of actions binding all firms, nor a case-by-case trade-off of commercial and ethical considerations, but a *layered approach* with policy principles (for

ICT companies are the lead players in huge social global change. They have more knowledge and more expertise than anyone else. They know about the technology and what the likely impacts are. They must take responsibility in anticipating the issues and trying to create ways of dealing with them.

Christopher Marsden
Chair of Amnesty's Business Group

example, how to respond to government or commercial pressure) at collective level used to inform local strategy formation and implementation.

Virtual worlds and crimes

The transformative nature of the Internet has raised another set of challenges, as aspects of social life are not merely conducted via the Internet, but have settled there in new forms exemplified by 'virtual worlds' (eg, Second Life) and massive multiplayer online role-playing games (MMORPGs, e.g. World of Warcraft).

- What or who defines 'crimes' committed wholly in cyberspace?
- Who or what, in the self-organised Web 2.0 world, is entitled to the virtual equivalents of humanity, citizenship or official authority?

2.3.2 'Web 2.0'

The next phase of the Internet's socioeconomic evolution is likely to be characterised by distributed applications and services and increasingly powerful networked computing.¹⁸ This 'unprecedented period of user interface innovation, as web developers are finally able to build web applications as rich as local PC-based applications' is referred to as 'Web 2.0'. (O'Reilly 2005) In particular, user-generated and distributed content may be central to consumers' Internet experience. (Benkler 2002; Benkler 2006) Like the Internet itself, stakeholders can route around obstacles, in the process making new connections and expanding demand in ways that make the totality even more indispensable. This ubiquity increases both potential commercial returns and the competitive forces, including 'non-commercial' competition, that dissipate them. This has three implications:

1. the 'client-server architecture' of both formal and informal governance is becoming more symmetric;
2. intermediation and content filtration services are increasingly separated (unbundled) from access or communication services.
3. the pace of change of social relations on the Internet is accelerating.¹⁹

Examples of rich Internet-based networking applications confirm this trend towards user-led innovation.²⁰ The vibrancy of these developments is exemplified by their variety and even more by their Protean uses and connections, including:

- P2P content sharing networks;
- blogs or online diaries;
- Wiki-based authoring, educational and reference resources;

¹⁸ 'Ajax incorporates: standards-based presentation using XHTML and CSS; dynamic display and interaction using the Document Object Model; data interchange and manipulation using XML and XSLT; asynchronous data retrieval using XMLHttpRequest; and JavaScript binding everything together' Garrett in O'Reilly (2005)

¹⁹ For instance, the founders and executive management of late 1990s 'Web 1.5' era companies now pass on commercial and technical experience to the new 'dot-com' boom.

²⁰ The Wikipedia citation for Web2.0 warns against over-hyping the term, but offers useful guidance on the content of such applications and services: see http://en.wikipedia.org/wiki/Web_2

- social networking for business (LinkedIn, ASmallWorld) and community (MySpace, FaceBook, Bebo) life;
- sites fundamentally based around user-generated content sharing (Flickr, YouTube).
- ‘data mashing’ – innovative ‘recombinant’ uses of existing media.²¹ Examples of data-mashing include the integration of maps with other information, and remixed music tracks.²²

Time and a progressive realignment of business models, user participation and shifting regulatory constraints will prove whether user-generated media is a forerunner of other user-generated or user-provider collaborative innovations or will be dominated by the ‘product’ generated within the commercial side of the content industry.

Although there is a lot of hype with the whole "web 2.0" phenomenon - there is very interesting activity around it - and ultimately and ideally, the potential for shaking up what we know and how we know it. Indeed, many entrepreneurs and academics alike feel that this is just the beginning.

Colin M. Maclay

Managing Director of the Berkman Center for Internet & Society

Web 2.0 also raises the issue of *inappropriate user-generated content*. Conventional labelling and rating methods may not be easily applicable. The legitimacy and acceptability of intervention raises ethical as well as practical questions.

- Who has the right to judge whether particular content should be shown or not?
- When does the intervention amount to inappropriate or unethical censorship?

Vivid examples show both sides of the debate, but the most successful responses share some multi-stakeholder elements. In the UK, there is a broad consensus amongst the public, regulators and some commercial ISPs that child pornography is clearly illegal and harmful and thus that BT’s successful introduction of a content blocking system for child pornography is both legitimate and necessary. The Internet Watch Foundation represents a more overtly multi-stakeholder and transparent approach to identifying content to be blocked.²³ However, the engagement of multiple stakeholders can institutionalise a failure of collective will, as in the compliance by Internet content providers with the Chinese

²¹ A term used in relation to the Internet only since 2004, see Wikipedia, itself an exemplar of user-generated content: http://en.wikipedia.org/wiki/Mashup_%28web_application_hybrid%29

²² This raises IPR issues over and above the ‘standard’ responsibilities of ICT industry players in protecting content creators’ moral and economic rights. Description and protected uses constitute distinct parts of formal patent protection, but are largely absent from copyright. As a result, the status of new and combined uses, e.g. the division of rights between original right-holders and ‘mashers’, remains unclear.

²³ The Internet Watch Foundation is an independent organisation established in 1996 following an agreement between government, police and ISPs aimed at reporting child abuse images and other illegal content, <http://www.iwf.org.uk>

government's demand to block a range of websites hosting political as well as sexual content.²⁴

Technology and social standardisation are two-edged: blocking systems established to inhibit access to content (and communication) can be used to serve the interests of the few as well as the many. Against this complex background, some companies emphasise that it is not possible, or even desirable, for them to take over the role of 'Internet police'. This is particularly true when the separation between the various functions:

- legislative – determining what is acceptable and expressing this in laws or norms;
- executive – enforcing acceptable behaviour through prevention or evidence collection;
- judicial – interpreting laws and norms in light of evidence and acting to impose sanctions

is unclear, or where the functions overlap across technological, market and jurisdictional boundaries.

Zittrain (2003) suggests that governments requiring ISPs to block and therefore censor content should 'be careful what you ask for'. It is important, to encourage legitimacy in the final decision and its observance, that all stakeholders ensure they are engaged in the discussion.

Such pressures impose devolved law enforcement responsibilities on hosts and/or providers in much the same way as government censorship demands impose political enforcement liabilities. While such stakeholders do not have the standing to accept these responsibilities, they may not have the power to resist them. There is, therefore, a clear need for them to develop a fundamental and explicit strategy in response to such pressures, to avoid the inconsistencies and ultimate failure of case-by-case approaches whereby the parties can be played off against each other.

2.3.3 Privacy and identity

Given the importance of secure personal data, legal and regulatory provisions relating to privacy of information, communication, physical space, civil liberties, etc. are clearly necessary. Private, technical solutions, while often more effective, sometimes undermine publicly driven privacy regulation, although not always, as shown by the recent TK Maxx incident shows.²⁵

²⁴ Although the most prominent example, China is not the only country censoring the Internet, as a recent six month study investigating into potential internet censorship in 40 countries revealed. (Waters 2007) In such cases, the ICT sector does not endorse, but merely enforces host country standards, and the weakness of the collective derives in part from commercial pressures, reinforced by a hope that such restraints will eventually become untenable as the Information Society unfolds. Of course, such 'soft-power' approaches are not limited to socially beneficial content.

²⁵ Hackers stole information from at least 45.7 million payment cards used by customers of US retailer TJX, which owns TJ Maxx, and UK outlet TK Maxx. (BBC News 30 March 2007:<http://news.bbc.co.uk/1/hi/business/6508983.stm>).

The concept of privacy as a fundamental right will change; driven by security concerns, transparency requirements and the benefits that people are rewarded for sharing information

Ian Goldin

Director of Oxford University's James Martin 21st Century School

Meeting such security challenges while remaining competitive and law-abiding is particularly challenging for global ICT companies. Privacy, only recently recognised as a fundamental human or economic right, is changing. Data security privacy is governed by:

- legislation;
- regulation;
- self-regulatory measures;
- organisational and individual approaches.

The range, amount, value and durability of personal data are expanding, driven in part by the growing reach of transactions. As the value (in exchange) of these data increases, business data holders face increasing pressure to protect others' data, and data subjects face increasing pressures to release or trade away such data. Both sides have little choice but to accept growing risks. The vulnerabilities and risks associated with distributed data could inhibit economic growth and participation, but could equally trigger a multi-stakeholder response.

Issues of privacy

- Privacy is relative – behaviour that might seem invasive or indiscreet to some is simply a fact of modern life to others.
- Privacy protections can keep people in as well as out, e.g. where people are denied access to services because they cannot give informed consent.
- Trades of privacy for other gains may not be required, proportionate, conscious or suitably optional.²⁶
- Privacy concerns and protections also differ by: geography; age; the ICT functions; types of data; who is involved.

People can, and increasingly do, interact with others in online communities where they can choose to share personal information freely and to project designed personalities.²⁷ This is

²⁶ 'Loyalty card' data are not required for purchases, and the available 'discount' need bear no relation to the value accruing to the store or given up by the consumer. The profile belongs to the store and inhibits consumer search. Consumers' identities may be linked to data they did not create or agree to withhold, as a result of profiling, identity theft or confusion. When records include data, or evaluations based on data (eg, credit decisions), legal protections may not restore accuracy, transparency or informed consent.

²⁷ This issue of choice lends weight to both identity and cybercrime issues. It may be hard for someone to separate an online identity from the core of their self-image and thus to 'get over' attacks or loss of identity. Similarly, studies of the welfare impact of societal isolation (e.g. Putnam, 2000), indicate that the ability to know and to choose associates is vital to both happiness and willingness to participate in communities. With

exemplified by social networking. People exchange information to enhance their social interaction and explore aspects of their own identity in potentially ‘low-risk’ ways. However, key aspects of identity, such as age and gender, cannot be verified, leading to concentrated risks exposing users to a range of real and virtual, but no less painful, crimes. The ‘real-world’ legalities are especially complex for minors; a US court dismissed a negligence lawsuit against MySpace by the family of a minor who was sexually assaulted by someone she met online. (Carlson 2007)

Private space, private property and identity are being redefined: interactions will become more open; less of what is now thought of as private will remain so in the future. But there may be substantial rebounds in the form of lost contact with:

- those unable to exercise increasingly complex controls;
- those unable to trust increasingly automated systems;
- ‘refuseniks’.

Trusting the systems

- Trust between humans differs from trust in machines or organisations.
- Suspicion may focus on accident, mistake or attack.
- Errors may involve false acceptance, false rejection or irrelevant imposition of information access or identification requests, etc.

The impacts on participation and on participants’ behaviour are likely to be complex.

Online communities of interest establish their own rules and culture spontaneously, based on their common values and preferences – these may complete or conflict with those in the off-line world.

The accumulation, exchange and processing of data by government agencies and businesses gives rise to new concerns about *civil liberties*. Recent security concerns have increased the stakes on both sides and, driven by pre-emptive policy actions, shifted emphasis to the government sphere.²⁸ In the post-9/11 world, governments have been prompted, and permitted, to collect, monitor and use much more personal information. This provides the appearance, and in some cases the effect, of enhanced security. However, the extent cannot be verified; the purposes expand, and there may be profound rebound effects, such as:

- reduced emphasis on other forms of policing;
- displacement of proscribed or dangerous behaviour to less-visible channels;

informed consent, these choices can be empowering, engaging and welfare enhancing; without it, they represent uncertainty and unmanageable complexity.

²⁸ This shift in relative emphasis does not mean that concerns about private sector invasions of privacy have lessened in absolute terms – as witness the controversies surrounding compromise of sensitive financial databases held by major financial and retail institutions (privacy of information and transaction) or around unsolicited commercial communication (privacy of personal space).

- the weakened self-protections of a surveillance society in which untrusted people trust less and become less trustworthy.

Increasing pressure on ICT firms to support these activities could provide a sense of proportion and a moderating influence on governments, if approached in the spirit of multi-stakeholder partnership. The ICT firms could require financial and regulatory compensation from the collective, or they could expand commercial exploitation of the information they are required to collect, store and provide.²⁹ The former course might encourage governments to consider whether such measures are, in fact, warranted. We do not suggest that collective or national security concerns are either trivial or exaggerated; merely, that they should not automatically trump individual and commercial interests. Appropriate decisions require appropriate feedback.

Moreover, international differences add to legal and operational complexity for global companies. Global ICT companies have to balance openly a range of varying government data collection and retention requirements against their own privacy policies and data protection obligations. Google's recent, qualified pledge to anonymise personal web search data after 18 to 24 months may be an attempt to pre-empt government action, but faces criticism from both sides.³⁰ The costs and benefits will only emerge after governments, other service providers and the public clarify their joint and separate responses.

As privacy is redefined and new forms of data collection, storage and profiling are developed, the rules for protection, for instance for personal interests and wealth, may need to be adjusted. A fair balance between privacy and security requires a reallocation of responsibilities among all parties from government to individual users. This allocation reflects presumptions about vulnerabilities and competence.

Child protection and consent

Child protection raises issues such as:

- parental consent – parents as agents of children;
- presumed consent of the child – children as their own agents;
- child-oriented web sites used to collect information on parents – children as 'agents' of parents.

The EC is pushing the ICT industry to develop a code of conduct to deal with children-related issues. Similar considerations arise around the infirm and elderly and others incapable of meeting the 'gold standard' of individual responsibility. Future policy will probably require multiple actions by all stakeholders:

- legislative changes;
- industry self-regulation;

²⁹ Such approaches are potentially disproportionate and impose direct costs for collecting, storing and securing the data and indirect liability reputation risks.

³⁰ See the BBC news website 'Privacy bodies back Google step' 15 March 2007.

- awareness-raising;
- application of privacy-enhancing technologies (many ICT-related technologies can be either privacy-invasive or privacy-enhancing).

This is thus a classic example of the need for a multi-stakeholder approach.

2.3.4 Copyright

The ownership and use of intellectual property is an important aspect of legal protection. Not too long ago, makers of software programs, such as Napster, faced suit by copyright holders.³¹ Now social websites like MySpace (News Corporation) and YouTube (Google) risk the same treatment. Copyright holders claim the companies are responsible for copyright infringement by users who put up protected content. On the other hand, some experts argue that websites are protected in the USA by the 1998 Digital Millennium Copyright Act removal of liability if notification of infringement is followed by immediate removal.

Global network operators have to comply with the European E-Commerce Directive.(2000/31/EC) Under this, an intermediate host is not liable if:

- a) not initiating transmission;
- b) not selecting the recipient;
- c) not selecting or modifying the information transmitted.

This exemption is not valid if the host knows that the content is illegal, which has led to fractious disputes about implied as opposed to actual knowledge of infringement.³² A further development is driven by the recognition that the societal argument for IPR protection is based on costs, benefits, and models of content creation, sharing and use that are increasingly at odds with experience. As a result, the balance between restrictive monopoly and open access implied by the need to reconcile incentives and just return for creative endeavour with the societal benefit of wide distribution are shifting for:

- content owners and distributors – the Apple decision to sell higher-quality content without DRM for a slight surcharge; many content creators' use of P2P channels to build 'network' demand;
- content users – the diffusion of P2P across different socioeconomic groups;
- governments – open access to publicly-supported research and creative content.

³¹ Napster was the first widely used P2P music-sharing service. It enabled users to exchange their music easily, in MP3 format, over the Internet.

³² See the recent example from Belgium: Davis (2007) Belgian Court Rules Google Violates Copyright With News Excerpts, February 14, 2007.

2.4 Conclusion: Networking raises global governance issues

Most sectors of the information infrastructure are privately owned and cannot be controlled by governments deciding what levels of connectivity or security should be available. Companies and individuals ultimately decide:

- what levels of broadband speed they want;
- the broadband speed for which they will pay;
- the risk they will tolerate; and thus
- what level of security ‘interference’ they are prepared to accept.

It is important to consider the strategic *technological implications* of the various policy options. Return on investment is the key to ICT providers’ decisions to invest in NGNs, and a critical part of that decision is the consideration of whether the network is offered as a non-discriminating wholesale or retail network, or a ‘walled garden’.³³ These decisions, whether taken as a competitive strategy by the telecom operator or mandated by the regulator, are critical to network architecture.

In brief, networks can be built for pure speed or for safety/convenience/privacy, and there is a critical cost trade-off between these two poles: strategy determines technology, and not vice versa. As broadband networks and their security form the basis for the networked ICT applications that drive the Information Society, it is unsurprising that the governance of these networks is increasingly a subject for a broader public policy debate.

For the ISP as intermediary, the potential exists for future technologies of filtering to substantially change the local control of nation states over the global Internet. Before allowing states to partition the resource in this way, it is relevant to ask the following questions.

- Might the solution to existing harms damage the medium’s innovative capacity?
- Might attempts by the state to use intermediaries to control citizen use of ICTs produce adverse rebound effects?

The above discussion concentrates on the potential to avoid problems arising from ICT-engendered societal transformation, while not overlooking the potential benefits. The negative tone in the overall corporate responsibility discussion is a backlash against ICT evangelists and the millennial ‘talking-up’ of ICT as a solution to a broad range of societal problems in many parts of government and industry. It also reflects the framing of corporate social responsibility as both a counterweight to the self-interested, gain-centred behaviour presumed to rule an ‘irresponsible’ commercial environment.

However, the power of the Internet to refocus commercial and societal forces towards non-monetised gains, including the creation and refinement of human and social capital, and to remove barriers is equally important. It has also produced a transformation in the generation and dissemination of creative and scholarly content, providing access to

³³ The Chinese government requires this of its network providers, although using much simpler technologies. See Clayton et al (2006).

publication and dissemination through low-cost channels that do not have to be justified by immediate commercial or volume advantages. Of course, flooding the Internet with content may be counterproductive, but the platform for publication provided by ISPs also supports broad and inclusive editorial comment, user rating and other forms of quality filtration.

CHAPTER 3 **ICT companies and the wider policy environment**

Previous chapters related multi-stakeholder approaches and the concept of responsibility for ICT companies to issues arising from the key enabling, networking and intermediary functions of the ICT sector. Global industries and the ICT sector, in particular, face a rapidly changing environment in which many old ‘certainties’ cannot be relied upon and the impacts unfold throughout an increasingly complex and interactive system.

This chapter extracts some implications of the literature and interviews conducted as part of the background research for this ‘Hot Topic’, in particular:

- two meta-conclusions regarding the nature of the problem itself;
- the drivers to the societal approach;
- three responses to the problems in the form of three ‘actions’.

3.1 **Wider impacts of ICTs**

The background literature and interviews suggest two meta-conclusions relating to the scale of the challenges facing ICTs and the scope for addressing them:

1. the importance of layered responsibility;
2. adjusting global governance to the complexity of the Information Society.

3.1.1 **The importance of layered responsibility**

While stakeholders are in many cases sensitive to the broader implications of actions relating to intellectual property, privacy, security, etc., they are at the same time obliged to act in their own interests and those of their customers, investors and regulators. This does not reduce responsibility to an empty shibboleth – rather, it points the way to a layered concept of multi-stakeholder governance founded on global citizenship. If the wider consequences of actions can be clarified to key stakeholders and issues of coordination resolved, individual and collective interests can be aligned.

The diversity of perspectives in the literature and interviews indicates clearly why these problems have resisted solution and may even have worsened in rebound from efforts to address them (eg, strengthening DRM or liability for harmful or illegal content). The spread of ICTs has vastly increased participation of all kinds of actors in the system as a

whole, without corresponding increases in engagement with collective governance or in formal institutional and collective commitment to build trust, encourage participation and limit opportunism. The insights into privacy below (see 3.3.2) illustrate this clearly.

3.1.2 **Adjusting global governance to complexity**

The Information Society behaves differently now than it did when existing divisions among public-sector, private-sector and civil-society institutions, issues or responsibilities were established. Complexity combines sensitivity to small changes in some areas with resistance to concerted initiatives in others. It is therefore necessary to 'rewire' the speed, efficiency and effectiveness of global governance. For example, global outsourcing and access to information have altered the distributions of education and income and triggered global movements of capital and labour in ways that weaken links between local populations and governments and between firms and their employees, suppliers, customers and regulators. In a slower world, the blind forces of evolution could be relied on to adjust business and political models to meet such economic, political, cultural and environmental challenges.

Another important consequence of complexity is *emergence* – the spontaneous appearance of qualitatively different systems and mechanisms, which may lead to coordination failures or missed opportunities to build new forms of engagement. These engagements are typically enhanced by ICTs, networking and joined-up working within and across private and public entities. For example, business increasingly tries to combine efficiency in meeting customer needs with consumer-centric partnership to:

- identify new needs;
- align customers' and businesses' holistic long-term interests.

The commercial and societal contributions of business activity have been transformed by:

- expanding personalisation;
- shared access;
- more explicit long-term relationships.

The public sector is shifting to:

- incentive-based regulation;
- increased awareness of the potential advantages of 'light-touch' regulation.

Civil society is also changing with:

- the formation of new issue-based or interest-based networks facilitated by ICTs.³⁴

³⁴ Witness the email, cell phone and web co-ordination of the fuel protests in 2000; the anti-globalisation protestors; and the emergence of the 'blogosphere' as an important forum for societal discourse.

It should not be assumed that these changes are necessarily good; they can be two-edged (*rebounds*):

- the information that lets a given retailer 'customise' its offering to the customer belongs to the retailer, so the customer would lose the benefits if s/he bought from a rival;
- technological change that enhances energy efficiency also decreases input costs and thus encourages use of scarce resources;
- strong collective mechanisms for assuring identity or protecting privacy can 'crowd out' individual precautions;
- the spread of blogs and other means of democratic expression can increase the scope for mischievous 'cheap talk' and excuse the introduction of enhanced restrictions.

Changes for the worse?

- The passing of old certainties opens the door to new forms of opportunism and conflict.
- Increasing contact among previously separated groups breeds new enmities.
- Possibilities for misunderstanding and mis-coordination increase with the complexity of individual decisions and the systems through which they interact.

3.2 Approaches to social change: drivers

It is useful to distinguish two related but conceptually distinct drivers of the societal approach to specific recommendations:

- incentives;
- selection or participation.

3.2.1 Incentives

If a private sector actor can address a problem with greater efficacy and lower cost acting of its own free will in pursuit of gain than acting under compulsion to avoid liability or penalty, it is socially efficient to ensure that the actor can anticipate suitable rewards. In the same way, if business participation in political or civil discourse helps inform debate and clarify available options, incentives for cooperative engagement should be protected, taking into account risks of collusion or anti-competitive behaviour.

3.2.2 Selection or participation

Any deliberative process benefits from the willing involvement of a wide range of stakeholders to ensure that:

- all interests are 'internalised';
- powers of action are suitably co-ordinated;
- defensive or aggressive responses by those 'left out' are guarded against.

On the other hand, a completely open process may be completely ineffective and, by seeming to address a problem, divert attention from effective solutions. Traditional mechanisms rely on a balance of compulsion and voluntarism but, especially in relation to the issues raised by the interviewees, it is essential to guard against a situation where ‘the best lack all conviction, while the worst are full of passionate intensity’.(Yeats 1920)

In a static world, the evidence described in the previous chapters would provide a blueprint for a new allocation of responsibility that would place responsibility on those best able to bear it and thus balance risk aversion against competence and knowledge. However, this view reduces responsibility to liability and does not encourage a *culture of societal responsibility* around collective issues. Instead, three kinds of action are suggested.

3.3 Approaches to social change: recommended actions

Three kinds of action, led by corporate global citizens acting in layered multi-stakeholder networks, are suggested:

- structural rebalancing;
- cross-cutting awareness;
- sector-specific policies.

3.3.1 Action 1: Structural rebalancing of roles and responsibilities

A structural rebalancing could take place through pro-active initiatives towards multi-stakeholder forums. To balance transparency and accountability with survival and efficacy, it is essential that:

- participants adopt norms of good practice;³⁵
- terms of engagement and reference are inviting and engaging;
- such initiatives be entrusted with serious responsibilities of their own.

Much is made of *convergence* in the ICT sector. Dynamics may force an allocation of responsibility where it can be leveraged and not where it is due. While it may be obvious that responsibility for harmful or illegal content *should* lie with those who knowingly make such content available, they are:

- numerous and widely spread;
- unknown to authorities;
- often motivated by non-monetary objectives;
- often immune to country-specific legal sanctions.

³⁵ Norms could be based on business principles outlined by Business for Social Responsibility available at: <http://www.bsr.org/CSRResources/IssueBriefDetail.cfm?DocumentID=48977>

Service providers might seem an attractive alternative, being close enough to content providers to observe and sanction their actions, and close enough to law and commerce to respond to simple sanctions and rules. However:

- service providers may have stronger incentives to offer qualified immunity to content providers;
- the market may separate responsible ‘walled gardens’ from an uncontrolled free-for-all fringe with no net solution to the problem.

The problem reflects *vertical integration* between content providers and service providers:

- the incentive effects drive convergence;
- the selection effects produce divergence or fragmentation.

The problem may be exacerbated by *horizontal linkage* of search engines to sites offering fraudulent, pornographic or other pop-up content or other malevolent activities that attach themselves to legitimate ICT services.

In addition, mixing of different cultural attitudes to broad societal goals could damage responsibility and accountability. For instance, in communications regulation of broadcast and telecommunications convergence, the antecedent sectors made different assumptions about control and choice and placed responsibility in different places. Convergence by market entry, merger or new hybrid business models and entities blurs lines of accountability.

3.3.2 Action 2: Raising the profile of cross-cutting issues

The second type of action involves *awareness-raising* around essential cross-cutting issues, such as:

- privacy;
- identity;
- intellectual property rights (IPRs);
- jurisdictional overlap;
- global political and security challenges.

These issues are important in a range of policy contexts and themselves form the hub of stakeholder networks that participate in shaping and implementing both formal and informal policy. Nonetheless, there are good reasons to suppose that current alignments of responsibility are less than perfect, and that the rebalancing of roles recommended above can only be attained if these externalities are addressed. In keeping with the multi-stakeholder perspective, the relevant actions include:

- participation in and organisation of a range of forums for collective activity;
- incorporating cross-cutting concerns into external (market, regulatory) transactions;
- increasing their visibility and salience in internal decision-making.

There is considerable debate about whether privacy is a right or an entitlement, and whether privacy is best viewed as:

- essentially transferable and monetisable economic rights – e.g. Fair Information Processing Principles; or
- inalienable human rights – e.g. OECD Privacy Principles.

As indicated in Chapter 2, privacy is an inescapable responsibility of ICT service providers acting as economic information intermediaries, and ranks high among essential human rights affected by their operation. Beyond individual companies' direct responsibilities and societal constraints, interactions with other entities raise further societal concerns. For instance:

- key decisions about identity technologies and exchange of personal information are often made tacitly on technical grounds or are closed to scrutiny and debate;
- a communications company may not directly infringe privacy or security but may facilitate information transmission, collection and processing in ways that do.

Such firms may also be best placed to understand developments in this area and act to mitigate threats or capture opportunities. Particular mention should be made of the risk of:

- 'contributory infringement' via commercial relationships that facilitate access to harmful or illegal content;
- IPR infringement;
- fraud.

The terms on which ICT firms engage with each other, content providers and end users rarely specify these matters in detail, and monitoring and enforcement are costly, difficult and fraught with their own perils. Issues such as 'net neutrality' are really forerunners of a more profound debate about responsibilities in respect of the use made of ICT services.

ICT firms operate in global contexts, spanning jurisdictions. This raises *compliance and engagement* issues:

- balancing obligations across global markets;
- dealing with the impact of globalised economic activity on, for example, labour and political conditions.

Specifically for the ICT sector, access to information plays a vital role in *governance*. Democratisation depends on open and unscrutinised access to reliable or at least diverse information and opinion. Repressive governments always seek to limit information access, while irresponsible use of communications threatens even democratic states.

ICT and the 'War on Terror'

The current threat from terrorist activity is bound up with public communication that mobilises forces on all sides, coordinates activities and drives political debate and decision. The response often involves collection and analysis of an unprecedented range of communication information. The 'War on Terror' has the potential equally to be won or lost on the battlefield of beliefs, ideas and expectations, or in physical locations. It is thus inevitable that the sector(s) that underpin and manage this contested area should be brought squarely into the conflict.

The range of issues is too vast for any one firm and the possibilities for gaps, duplication or working at cross purposes are broad. It is thus essential to frame and clarify the issues in a multi-stakeholder context, and to develop collective policies, especially for use in dealing with the asymmetric power of host governments.

3.3.3 Action 3: Specific for sector policies

The final type of activity is focused on specific policy areas identified in interviews:

- privacy and communication rights;
- digital divide;
- security and reliability.

Privacy and communication rights – ICT and other companies should foster collective action by:

- introducing improved accountability mechanisms;
- linking corporate and public policy;
- joining with Non Governmental Organisations (NGOs), and international agencies, etc. to:
 - create standards;
 - exchange good practices;
 - establish transparent processes.

They should engage with policy makers and supranational entities to increase leverage on these issues, taking key roles in:

- privacy regulation;
- self-regulation;
- technology development;
- policy debate;
- implementation (legislation and regulation).

In many cases, problems arise with those who collect and exploit information rather than those who process or transmit it. The central role of ICT companies ideally suits them to drive research and debate on:

- essential privacy rights;
- the force of informed consent;
- the deeper question of ownership of personal information.

Moreover, because ICT companies at present receive government (and other) data requests and provide strategic information processing, storage and exchange services, they can enforce collective standards and gather necessary information about the prevalence of infringement, ‘mission creep’ and the like.

Digital divide – the digital divide separates Information Society ‘insiders’ from both willing and unwilling ‘outsiders’, and initiatives should address both populations. While increased access suffices in most cases to engage the latter, the former may be harmed by inclusion, especially if:

- their skills and understanding do not keep pace with technical possibilities;
- their needs and abilities are not taken into account.

The Internet is an ‘experience good’, and time and experience are required to appreciate it. It should not be assumed that all should participate or that all should participate in the same way – thus it is necessary to involve far more than providers of ‘basic services’. Both individuals and communities must be represented, since individual demand is not the same as societal welfare – as experience with online gambling clearly demonstrates.

The ‘digital divide’ is also part of a broader picture of deepening inequality and disadvantage. This reflects in part the economic ‘tipping’ characteristics of ICT-led economic development and in particular expanded awareness of conditions affecting others.³⁶ Because countries and other groups of people differ in skills, cultural perspectives and societal infrastructures, ‘equalising growth’ is not an inevitable consequence of opening markets and making technology available. ICT companies could collectively support schemes to deliver health and education services in ways that build necessary skills and judgement as a by-product, and actively work to develop solutions to imbalances of global demand and supply that favour sustainable, divide-reducing growth over the winner-takes-all dynamic.

Security and reliability –Telecommunications and IT services companies like BT play a crucial role in security and reliability. They own/operate the infrastructure, must juggle government demands to make the CNI (Critical National Infrastructure) as robust and reliable as possible, but also have to meet investor and business objectives. The sector as a whole should strive to include security amongst its objectives. In the short term, this could mimic ‘triple-bottom-line’ accounting (i.e. covering the three dimensions of sustainability: social, environmental and economic) used to spearhead sustainability. Given concrete

³⁶ ‘Tipping’ is the tendency to concentration of market power and international, educational and other inequalities.

action to introduce visible improvements, markets (starting with financial and insurance markets) will come to recognise and value trust and confidence.

3.4 **Conclusion: Leading the responsibility agenda**

Traditionally, the analysis of issues would lead to a re-allocation of responsibility to those best able to bear it and thus balance risk aversion against competence and knowledge. However, this reduces responsibility to liability and does not encourage a culture of societal responsibility around collective issues, nor take into account the nature and effects of complexity and associated emergence of new institutions, arrangement and engagements. It also ignores the practical tasks of defining and ensuring or enforcing compliance with societal norms in the context of the networked Global Information Society.

This suggests three kinds of action:

1. structural rebalancing of roles and responsibilities;
2. raising the profile of critical cross-cutting issues;
3. targeted response in specific domains where ICTs play a crucial role in enabling socio-economic development and change.

As a key player in the global ICT sector with a global reputation as a leader in the CSR domain, BT has an important role to play in leading this responsibility agenda. We will discuss specific recommendations for BT in the final chapter.

Real leadership is about doing something because you know it is the right thing.

Kenneth Cukier

Technology correspondent for the 'The Economist'

The purpose of this concluding chapter is to spell out some additional recommendations consistent with BT's overall strategic engagement in embracing responsibility at all levels of the multi-stakeholder agenda, especially in the areas of:

- exercising leadership in external forums;
- incorporating issues such as sustainability into its own decisions.

4.1 Options for BT in redefining multi-stakeholder governance

4.1.1 Realigning responsibilities

The report notes the similarity between responsibility and risk, and thus the importance of a risk-allocation perspective. A global ICT provider acting in this area acts as an agent of:

- society at large;
- those stakeholders to whom it owes ethical or legal duties of care.

These explicit or implicit social contracts must fit into BT's network of financial and legal contracts. As the existing assignment of responsibility may differ from the optimal assignment or distribution, BT has opportunities to act in relation to its responsibilities while at the same time working to clarify and implement an appropriate realignment.

The current power geometry helps to classify BT's position with regard to its responsibilities and its ability to influence reallocation of roles within the ICT sector. The responsibilities are those:

- BT is best-placed to discharge;
- projected onto BT – due to size, visibility, political and commercial burden-shifting or desperate hope – but not best discharged by it;
- fixed at the individual firm level – BT in particular;
- defined or imposed at the sectoral level or higher.

The policy and societal interests involved are closely intertwined. The key message remains multi-stakeholderism, applied both internally and externally:

- internally – the engagement of BT responsibility with other business units as both a sponsor of responsibility concerns and a platform for discussion and coordination;
- externally – engagement with a range of forums of varying composition and formality.

This can:

- enhance effectiveness;
- minimise the adverse commercial and sustainability consequences of coordination failures;
- enhance trust by removing any suggestion of special pleading.

4.1.2 The sustainability challenge

BT is well placed to continue, internally and externally, its multi-stakeholder engagement with sustainability and its useful critique of the increasingly inadequate conventional framing of sustainability, described in Chapter 1, 1.4.

Leadership is also essential in this area. BT's opportunity in this respect is enhanced by having taken the lead in incorporating sustainability into its own operations and 'spreading the word' through active engagement with other ICT players and, to some extent, civil society, thus helping set the responsibility agenda. This suggests a next step of engagement with and through the regulatory process: self- and co-regulation and incorporation of sustainability concerns into regulation.

4.1.3 BT and regulatory relationships

BT's regulatory relationships give it, and other producers of services similarly regulated by formal bodies and market forces, a central role (see Figure 3 for a simplified view).

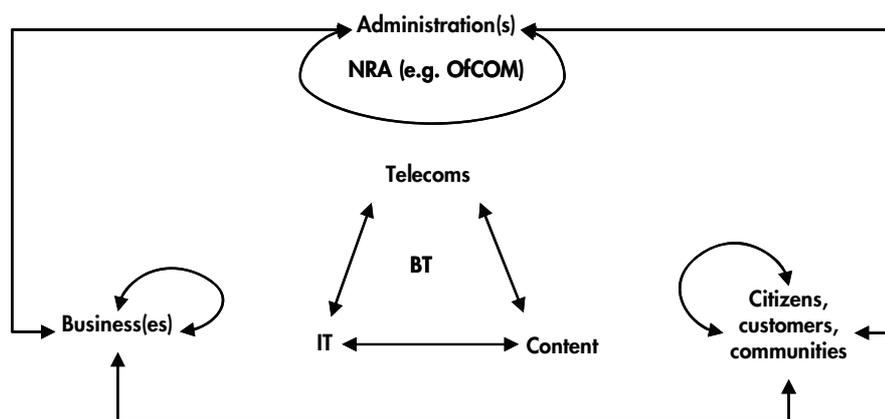


Figure 3. Schematic representation of BT's central role and its regulatory relationships

Within the central ICT triangle, BT has a particularly broad range of choices of role:

- ‘mere’ network provider;
- integrator;
- market broker connecting the other parties.

In addition, as a key informant for the converged communications regulator in the UK (OFCOM), and thus a trusted intermediary in the relations between regulation and the ICT sector in general, BT can act as a focal point for co-regulation. Alternatively, BT can support an enhanced role for the regulator as a facilitator in aspects of its charter outside its direct and traditional ‘hard power’ portfolio. For instance, industry convergence and the combined impact of a plethora of legal rules increase tensions between technical, economic and social regulation.³⁷ The *de facto* partnership of the converged regulator and the pre-eminent incumbent forms the joint apex of these clusters.

To develop this choice of roles requires a basis for weighing the alternatives and drawing on other areas of investigation.³⁸ Development is driven by shocks on one side and different speeds of adjustment on the other. ‘Institutionalised’ (slow to change) aspects add commitment power and may make overall evolution more coherent, but can also store up trouble and thus breed crises. BT’s choice of role translates into a set of commitments to act strategically in some areas and responsively (reactively) in others.

4.2 Conclusion: Some ICT-specific recommendations

We conclude with two specific recommendations to BT as corporate citizen and exemplar. These acknowledge the dichotomous nature of foreign engagements.

1. ICT companies can extend their sustainable operations down the supply chain by:
 - undertaking pre-contract assessments in developing countries;
 - supporting and educating suppliers to provide sustainable services;
 - taking a closer look at the activities of suppliers, particularly in offshore Business Process Outsourcing (BPO), to see that they are not in breach of applicable regulations and legislation in their host country.

BT currently takes a lead in such assessments, especially in the post-contract phase, where it involves direct involvement of key stakeholders. This could usefully be extended into the pre-contract phase, when a broader set of stakeholders can be engaged. BPO in particular carries ethical responsibilities for labour conditions and societal impact on host countries, which are magnified for ‘weightless’ ICT enterprises that are less embedded in the local economy. BPO enables companies to use commercial terms and conditions to reinforce

³⁷ For example, at European level, the ONP, eCommerce, AVMS, Copyright and Privacy Directives.

³⁸ For example, the changing composition of society: the overlapping mappings of people, institutions and ‘focal issues,’ and the analysis of so-called ‘policy networks’.

sustainable economic development, especially in respect of profits returned to the developing countries in question and ethical labour conditions.

Such decisions have competitive consequences, so BT should consider this a strategic opportunity to 'raise the game' of the ICT sector and slow or reverse the 'race to the bottom' cited by critics of globalisation. Public procurement rules also make some allowance for incorporation of sustainability and related concerns in public tender specification and evaluation and simultaneously for variants in bids. BT plays an active role in this market and could thus use invitations to tender to advance the responsibility agenda in a market segment that constitutes some 16% of European GDP.

2. BT can exercise 'ethical leadership' in its direct overseas activities in dealing with host governments, International Financial Institutions, and other global businesses. Responsibility, in global ICT companies, requires:
 - clear objectives;
 - reporting achievements against these objectives; and
 - integrated decision-making that reflects the interests of a multiple stakeholders

The underlying ethical question here is whether the telecommunications and other services thus provided will advance development or be used instead to suppress dissent, in which case the company would have to explore which tenders to bid for (integrating ethical concerns into what is essentially a commercial judgement) and perhaps whether the supply of services might give some 'leverage' over the ethics of clients' behaviour.

Building responsibility into corporate strategy ensures it is not an afterthought, bolt-on or one-off action and thus increases policy efficacy and leverage. Sustainability information is obviously relevant and must be visible and integrated into responsible commercial decision making. By the same token commercial considerations must be taken into account when analysing and adjusting sustainability strategies. BT is actively engaged with a variety of fora with different constituencies, objectives and instruments. BT should consider in light of visible differences between e.g. NGO and corporate participants (e.g. around codes of conduct) that inhibit collective solutions could be addressed by an integrated strategy across BT's external engagement and commercial strategies that could help all participants to share in progress towards a common interest in advancing the sustainability agenda. Internally, we note that sustainability concerns, once reflected in a dedicated section of BT's annual report, are now increasingly reflected throughout the report. This reporting integration enables BT to communicate the interaction of commercial and sustainability concerns to its Board, (current and potential) investors and other stakeholders. But this is of limited utility if sustainability and commercial reporting only appear together when the reports and accounts are signed off – ideally, this integrated reporting should be used to support a further integration of decision-making on commercial and 'responsibility' strategies. This development can also enhance current efforts to elicit the views of external stakeholders in order to ensure that their views are suitably reflected in objectives, decisions and strategy and to improve mutual understanding throughout the multistakeholder community.

REFERENCES

Reference List

- Benkler, Y. 2002. Coase's penguin: Or linux and the nature of the firm. *Yale Law Journal* 112.
- Benkler, Y. 2006. *The wealth of networks: How social production transforms markets and freedom*. New York: Yale University Press.
- British Computer Society. Broadband security: Managing the risks. <http://www.bcs.org/server.php?show=conWebDoc.1506>
- Brown, I., L. Edwards and C. Marsden. 2006. Legal and institutional responses to Denial of Service Attacks. Joint seminar on Spam/DdoS, Communications Research Network/Department for Trade and Industry, 13 November. <http://www.communicationsresearch.net/events/article/default.aspx?objid=1464>
- Brundtland Commission. 1987. *Our common future*. The World Commission on Environment and Development. Oxford: Oxford University Press.
- Carlson, N. 2007. Judge faults parents in MySpace sexual assault suit, February 15. *Internetnews*. <http://www.Internetnews.com/xSP/article.php/3660286>
- Cave, M., L. Prosperetti and C. Doyle. 2006. Where are we going? Technologies, markets and long-range public policy issues in European communications. *Information Economics and Policy*, 18:3 242–255.
- Clarke, D. 2005. FIND and architecture: A new NSF initiative. http://find.isi.edu/presentation_files/Clark_Arch_Security.pdf
- Clayton, R., S.J. Murdoch and R.N.M. Watson. 2006. Ignoring the great firewall of China. Paper presented to the sixth workshop on Privacy Enhancing Technologies, Cambridge, UK, 28 June.
- COM. 2006. 136 Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee. Implementing the partnership for growth and jobs: making Europe a pole of excellence on corporate social responsibility. http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0136en01.pdf
- Davis, W. 2007. Belgian Court Rules Google Violates Copyright With News Excerpts, February 14. http://publications.mediapost.com/index.cfm?fuseaction=Articles.showArticle&art_aid=55512

- Digital Opportunities Task Force. 2001. Digital Opportunities for All: Meeting the Challenge.
<http://lacnet.unicttaskforce.org/Docs/Dot%20Force/Digital%20Opportunities%20for%20All.pdf>
- European Commission. 2001. Green Paper - Promoting a European framework for corporate social responsibility. http://ec.europa.eu/employment_social/social/csr/greenpaper_en.pdf
- European Commission. 2006. 'Staff working document', 28 June, at: http://ec.europa.eu/comm/avpolicy/reg/tvwf/modernisation/consultation_2005/index_en.htm, at section 6.4, Net Neutrality
- European E-commerce Directive. 2000/31/EC of the European Parliament and of the Council. 8 June.
- European Multistakeholder Forum on CSR. Review Meeting, December 2006.
http://ec.europa.eu/enterprise/csr/forum_2006_index.htm
- Hoffman, J. 2005. Internet governance: A regulative idea in flux. Paper presented to European Consortium of Political Research, September, in Budapest, Hungary.
- International Telecommunication Union. 2005. The Internet of things. International Telecommunication Union Internet Reports. Geneva.
<http://www.itu.int/osg/spu/publications/internetofthings/>
- IPSphere. 2006. Creating a commercially sustainable framework for IP services realizing next generation revenues. Ipsphere, Forum Work Program Committee Version 1b.0, May.
http://www.ipsphereforum.org/home/IPsphere_CommercialPrimerExec050806.pdf
- Katagiri, Y. 2006 Japanese interconnection policy on NGN.
<http://www.oecd.org/dataoecd/6/52/37503176.pdf>
- Kleinwächter, W. 2004. Internet co-governance – towards a multilayer multiplayer mechanism of consultation, coordination and cooperation. Paper presented at the informal consultation of the Working Group on Internet Governance (WGIG), September 20–21, in Geneva, Switzerland.
- Kooiman, J. 2003. Governing as Governance. London: Sage.
- Kummer, M. 2004. The results of the WSIS negotiations on Internet governance. In Internet Governance, ed. Don MacLean, 53–57. A Grand Collaboration, ICT Task Force Series 5. New York.
- Lessig, L. 1998. Governance. Keynote speech at CPSR Conference on Internet Governance, October 10. <http://www.lessig.org/content/articles/works/cpsr.pdf>
- Lessig, L. 1999. Code, and other laws of cyberspace. New York: Basic Books.
- MacLean, D. 2004. "Herding Schrödinger's Cats": Some conceptual tools for thinking about internet governance. In Internet Governance, ed. Don MacLean, 73–99. A Grand Collaboration, ICT Task Force Series 5. New York.

- Marcus, J. Scott. 2004. Evolving Core Capabilities Of The Internet. *Journal on Telecommunications and High Technology Law*, 3: 123-163.
- Marsden, C. 2006. Next Generation Networks and the Last Mile Bottleneck: A co-regulatory solution? Forthcoming in *Telecoms Policy*.
- Mueller, M., J. Mathiason and L. McKnight. 2004. Making sense of “internet governance”: Defining principles and norms in a policy context. In *Internet Governance*, ed. Don MacLean. A Grand Collaboration, ICT Task Force Series 5. New York.
- OECD Foresight Forum. 2006. Next Generation Networks: Evolution and policy considerations. 3 October.
http://www.oecd.org/document/12/0,2340,en_2649_33703_37392780_1_1_1_1,00.htm
- O’Reilly, T. 2005. What Is Web2.0?
<http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html>
- Putnam, Robert D. 2000. *Bowling Alone: The Collapse and Revival of American Community*. New York: Simon & Schuster.
- Talbot, D. 2006. Toward a high-definition YouTube. *MIT Technology Review*, 26 October.
- United Nations. 2005. Report of the Working Group on Internet Governance. Transmitted to the President of the Preparatory Committee of the World Summit on the Information Society, 14 July. <http://www.wgig.org/WGIG-Report.html>
- United States 2006. United States Congress “Internet Freedom and Nondiscrimination Act of 2006”. http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_bills&docid=f:h5417rh.txt.pdf.
- Wadawsky, J. 2005. IMS 101: What you need to know now.
http://www.bcr.com/carriers/public_networks/ims_101_what_need_know_now_2005_061514.htm
- Waters, Richard. 2007. ‘Web censorship spreading globally’, *Financial Times*, at: <http://www.ft.com/netcensorship>.
- Yeats, W. B. 1920. “The Second Coming”. In *Collected Poems of W.B.Yeats*. London: Macmillan.
- Zittrain, J. 2003. Be careful what you ask for: Reconciling a global internet and local law. In *Who Rules The Net?* ed. A. Thierer. Cato Institute.

APPENDIX

Appendix: List of interviewees

EXTERNAL INTERVIEWEES

Kenneth Cukier	Technology correspondent for the ‘The Economist’
Ged Davis	Managing Director, Head of Centre for Strategic Insight, World Economic Forum
John Dryden	OECD Deputy Director, Science, Technology and Industry
William Dutton	Director of the Oxford Internet Institute, University of Oxford
Ian Goldin	Director of Oxford University’s James Martin 21st Century School
Mark Goyder	Director, Tomorrow’s Company, and member of BT’s Leadership Panel
Ayesha Hassan	Senior Policy Manager for E-Business, IT and Telecoms, International Chamber of Commerce
Dunstan Hope	Director at Business for Social Responsibility (BSR)
Hiddo Houben	Member of Cabinet of European Commissioner for Trade
Markus Kummer	Executive Coordinator of the IGF Secretariat
Colin M. Maclay	Managing Director of the Berkman Center for Internet & Society
Christopher Marsden	Chair of Amnesty’s Business Group
Jane Nelson	Director of Corporate Social Responsibility Initiative at the JFK School of Governance, and Director of Business Leadership & Strategy of the International Business Leaders Forum
Philippe Renaudiere	Head of Unit, Data Protection and Privacy, Secretariat General of the European Commission

BT INTERNAL INTERVIEWEES

Petri Allas	BT Group Corporate Strategy Director
Francois Barrault	BT CEO Global Services
Dave Brown	BT Foresight Manager
Tony Cox	BT Wholesale
Liz Cross	BT responsibility strategy and policy for procurement
James Freund	BT Market and Brand Team
Paul Kenny	BT Leader of the 21st Century Network
Angi Lewis	BT Wholesale
Mita Mitra	BT Group Legal
Susan Morgan	BT Sustainability Manager
Tom Mullen	BT Head of Security Investigation Services
Caroline Persson	BT European Affairs Office
Bruce Schneier	BT Counterpane
Chris Tuppen	BT Head of Sustainable Development and Corporate Accountability