ICT Policy: A Beginner's Handbook

Edited by Chris Nicol

Published by the Association for Progressive Communications - www.apc.org

Made possible with the support of the Commonwealth Telecommunications Organisation - www.cto.int

Published by the Association for Progressive Communications

Illustration: Matias Bervejillo, Montevideo, Uruguay

Graphic design: MONOCROMO, Montevideo, Uruguay

Printed by: STE Publishers, Johannesburg, South Africa

Address: PO BOX 29755, Melville 2109, Johannesburg, South Africa

ISBN: 1-919855-10-6

Website: www.apc.org

E-mail: info@apc.org

First published in 2003

This book is available at http://www.apc.org/books

Contents

Foreword

Information and communications are at the heart of human life and social development. People have always worked together by sharing information and knowledge through speech, writing, the printed word and, more recently, telephony and broadcasting. Sharing information empowers individuals and communities, and enables whole societies to benefit from the experience of everyone within them.

The last decade has seen major changes in our capacity to communicate and share information through new developments in information and communications technology, particularly the Internet. These changes offer tremendous new potential for effective communications, but their availability and accessibility to citizens and communities depends on decisions made by many people in government, business and civil society - decisions that often seem arcane, technical or specialist but which have profound implications for the future of society.

This book aims to guide non-specialists through some of these policy issues and enable its readers to engage effectively with the decision-making process. It came about through a partnership developed between the Association for Progressive Communications, the leading international civil society group on ICT policy issues, and the Commonwealth Telecommunications Organisations, during my term as the Organisation's Chief Executive.

That partnership was originally forged in the margins of the DOT Force, the influential multistakeholder forum on ICTs and development involving the G8 and a group of developing countries in 2000-2002. I am delighted that this particular product of multistakeholder partnership is now available and hope that it will prove a valuable tool for all involved in work to make new ICTs available and valuable for every member of the world community.

Professor David Souter
University of Strathclyde

Introduction

Ask a typical citizen about ICT policy and s/he will probably reply with a comment like 'what's that?' or 'who cares?' Getting involved in Information and Communication Technology (ICT) policy-making has not been a priority for most people, even those who are generally active in other areas of public policy. It often seems removed from our daily experience, and technically complicated. Yet new communications media are becoming so important that we cannot continue to ignore them.

This book takes the mystery out of ICT policy and makes it easier to understand. Key issues are presented and explained clearly and concisely, and a basis is provided for further investigation. Many concrete examples are given of recent events or debates, which the reader can explore further if so inclined. Having read it, you will be able to identify the main actors and issues in the field. If you wish to find out more about ICT policy, you will know where to look for the information, beginning with the extensive bibliography and list of organisations active in the field. In short, this book aims to build the capacity of interested persons to understand the issues around policy on ICT development and regulation, to grasp the policy process, and to become involved in it. It is a beginner's handbook, which can help readers navigate their way through the varied terrain of ICT policy. It is not a map but a compass.

While the area of concern includes many kinds of ICTs, our interest is centred on the internet. This network of networks is the most innovative and fastest-growing new technology, and has become vitally important to contemporary societies. Many of the more traditional ICTs are converging on the internet, using it, becoming part of it, and often becoming indistinguishable from it. The internet is still in its infancy, but powerful forces are trying to limit the freedom currently enjoyed by internet users. The future of ICTs is everyone's business, and APC would like ICT policy-making to be participatory, involve all sectors of society, and to benefit all, not just the powerful and the well-organised.

This book should thus be of interest to a wide range of people: members of civil society groups, researchers, activists, technical persons who are getting more interested in the political side, journalists looking for background information, government-administration workers, or anyone else who is interested in the topics. It is not a technical book, although it tries to explain in simple language some of the technical background knowledge that is necessary in order to be able to discuss and debate ICT policy issues.

The first chapter explains what is meant by ICT policy, and why it is important. It locates our interest in ICTs in a historical moment, when it is particularly important to ensure that the freedoms enjoyed by internet users are not eroded by restrictive legislation or practices, and that they are extended to all countries and citizens.

Part Two looks at what makes the internet different from other media and ICTs, and seeks to explain why present internet use is inequitably distributed. It explains how it is possible that internet access is more expensive in the countries whose citizens can least afford it, and is cheaper for citizens in wealthier countries. It calls for regarding internet access as a social issue and not merely an economic one.

Part Three explains policy and regulation, how policy is decided, who the main players are, and what can be done to ensure that policy decision-making is a transparent, participatory process, and not one which involves only those with the money and the power to influence governments and the courts.

Part Four considers specific themes in ICT policy, again with a special focus on the internet. These are topics of great interest, which will determine how our societies develop over the next 20 years, and we can and must intervene in them. While some important issues have been left out, the topics discussed here are crucial. Our aim is to make them easily understood by all.

The appendices are designed to help the reader understand some of the technical terminology, as well as continue the journey beyond the boundaries of this book. The list of organisations gives an idea of who is working in the field, and also how to get in contact with them. We hope that reading this book will stir your interest in becoming involved in current debates and campaigns, and that this list will help you do so. Finally, the bibliography suggests further readings to find out more on the many topics and issues referred to in the book.

The book has been produced by the Association for Progressive Communications with funding via the Commonwealth Telecommunications Organisation (CTO) from DFID's Building Digital Opportunities programme. Some of the material was adapted from APC's *ICT Policy Curriculum* (http://www.apc.org/english/capacity/policy/curriculum.shtml), but most was written specially for the book by Kate Wild, Russell Southwood, Natasha Primo, Paul Mobbs, Claire Sibthorpe and Chris Nicol (editor). The team of reviewers included Sonia Jorge, Anriette Esterhuysen, Carlos Afonso and Karen Banks. Additional editing by Ran Greenstein. Graphics were created by Matias Bervejillo and Piet Luthi (chapters 11 and 13). Special thanks to Karen Higgs and all those in APC (Heather, Danijela, PatchA and others) who helped with ideas, resources, and advice. Thanks also to David Souter, formerly at CTO, for his generous support, without which this book would not exist. ■

CHRIS NICOL

ICT policy / part 1

1. What are ICT and internet policies and why should we care about them?

1.1. Information and communication technologies

Information and communication are integral to human society. In many cultures today, information retrieval and presentation – the recording of wisdom and history – is still done with the use of speech, drama, painting, song or dance. The use of writing changed this enormously, and the invention of the printing press allowed communication on a massive scale, through newspapers and magazines. More recent technological innovations increased further the reach and speed of communication, culminating, for now, with digital technology. These new ICTs can be grouped into three categories:

- **Information technology** uses computers, which have become indispensable in modern societies to process data and save time and effort
- **Telecommunications technologies** include telephones (with fax) and the broadcasting of radio and television, often through satellites
- **Networking technologies**, of which the best known is the internet, but which has extended to mobile phone technology, Voice Over IP telephony (VOIP), satellite communications, and other forms of communication that are still in their infancy.

Information Technology

- Computer hardware and peripherals
- Software
- Computer literacy

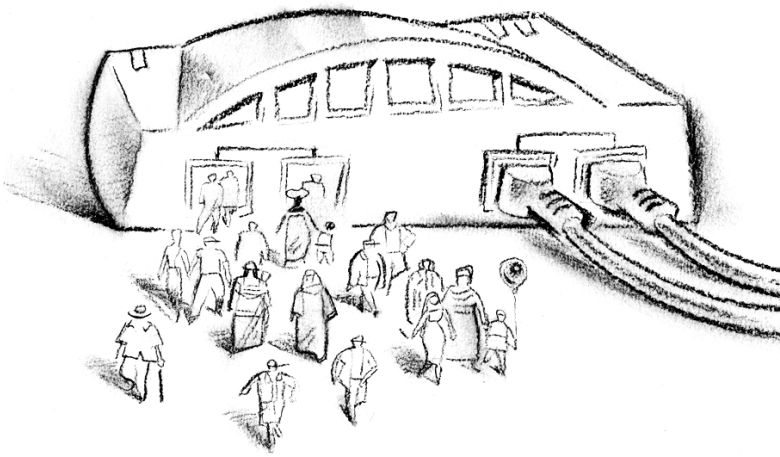
Telecommunications Technology

- Telephones system
- Radio and TV broadcasting

Networking Technology

- Internet
- Mobile telephones
- Cable, DSL, satellite and other broadband connectivity

These new technologies have become central to contemporary societies. Whether you are talking on the phone, sending an email, going to the bank, using a library, listening to sports coverage on the radio, watching the news on TV, working in an office or in the field, going to the doctor, driving a car or catching a plane, you are using ICTs.



Convergence

The new ICTs do not operate in isolation from one another. The advantages and reach of the internet make it a focal point for the use of new technologies. Its decentralised, widely-distributed, packet-based mode of transporting information makes it an efficient, cheap and flexible means of communication, which facilitates interrelationship with other technologies. So, for example, international telephone calls are increasingly made through the internet's network of networks, and television and radio are broadcast via the internet. Today's Local Area Networks must be connected to the internet and secure copies of data (backups) are now made through the internet rather than onto a local drive. Software, music and video can be rented through the internet, sometimes without even requiring a copy on the local computer. The internet is accessible through mobile phone networks, which use it to present content to the user, and digital movies will be soon distributed through the internet to cinemas. The list is long and getting longer by the day.

Not only are new technologies converging in this way, the areas where they are applied are also becoming interrelated. Telecommunications are firmly based on computer technology, and are fundamentally dependent on the internet. For example, the software that makes computers so useful is now often created by a team of programmers who may live and work in different countries, but can collaborate and communicate via the internet. Telephone companies are increasingly using VOIP to reduce their international communications costs. Consumer commodities too are becoming dependent on the internet. This is especially true of electronic devices and appliances, such as audio and DVD recorders and players, or refrigerators.

This convergence happens not only at a technological level, where everything is in bits (binary digital form) and the internet is the main way of moving this information from place to place, but also at the level of industry. These days, a large internet service provider will probably also be linked to a telecommunications infrastructure company, and have subsidiaries that produce software or own an internet search engine. The important media multinationals are buying heavily into internet technology as they see it as the physical and conceptual infrastructure for media in the future. This has led to a situation where telecommunication giants are also multimedia giants with huge investments in internet technologies. The same company that broadcasts your favourite TV programme may also be the one that allows you to access the internet, or provides your ISP with its connection to the rest of the internet. The movie you watch at your local cinema may well be produced by a media multinational that owns your local newspaper and also a telephone company that runs a main internet portal.

Convergence: the case of America Online Time Warner

Companies absorbed or created by AOL Time Warner:

- Internet service providers: America OnLine, Compuserve
- Software: Netscape, ICQ, AOI Wireless
- Television: CNN, HBO, Time Warner Cable
- Music (mp3), Warner Music
- Film and video: Warner Bros
- Magazines: Time, People, etc.
- Books: Warner Books, Little & Brown, bookstore chains, etc.

Convergence: the case of AT&T

Traditionally the long distance telephone operator in the USA, AT&T is now a major internet carrier and infrastructure provider, with four major sections: AT&T Broadband, AT&T Business, AT&T Consumer, and AT&T Wireless. It has expanded into the multimedia field by acquiring all or part of these companies:

- TV: Telecommunications Inc, Liberty Media Group (Discovery Channel, Encore, etc)
- TV Guide
- Broadband access and portals: Excite At Home
- AOL Time Warner (9%)
- News Corporation (8%)

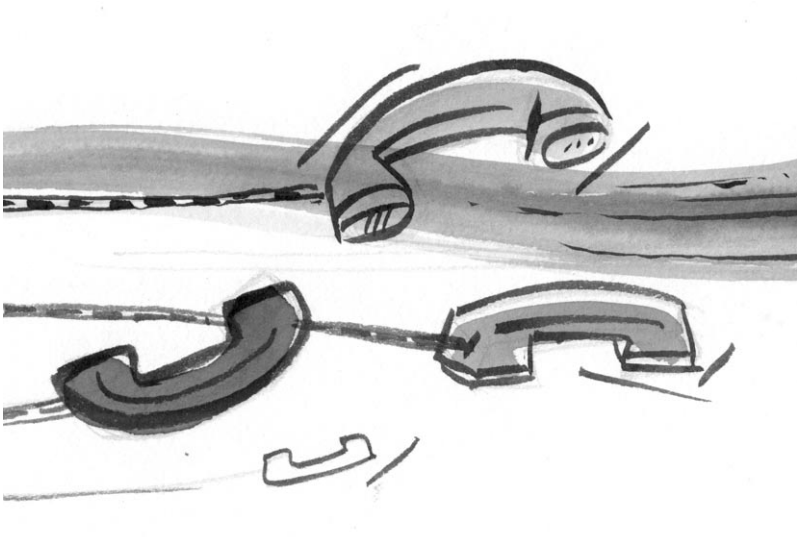
Source: TM McPhail, 2002.

If technology and industry are coming together around the internet, governments that decide policy and regulate industry must recognise this fact and adapt their policy-making accordingly. For example, there is no point in regulating traditional broadcasting in the usual way if it is being replaced by internet broadcasting which follows a different set of rules. The traditional regulation of broadcasting, involving restricted bandwidths, and huge investment costs, cannot be applied to new forms of broadcasting which require relatively little capital outlay, are instantly global and available to everyone, have open standards that facilitate access in multiple ways, and are decentralised so that coordinated control is very difficult. The notion of intellectual property and copyright changes when all information is digital and can be freely copied and transported. For example, legislation about recorded music must take this into account. Other questions arise: How should workers' rights to privacy in the workplace be regarded in the context of email and the World Wide Web? What will it mean to regulate telephone call costs when the ability to call via the internet at a much reduced rate becomes generalised?

1.2. What is ICT policy?

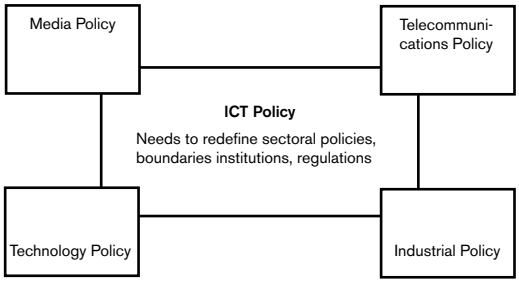
The Oxford English Dictionary defines policy as "A course of action, adopted and pursued by a government, party, ruler, statesman, etc.; any course of action adopted as advantageous or expedient." While this definition suggests that policy is the realm of those in power – governments or official institutions – a wider sense could include the vision, goals, principles and plans that guide the activities of many different actors.

ICT policy generally covers three main areas: telecommunications (especially telephone communications), broadcasting (radio and TV) and the internet. It may be national, regional or international. Each level may have its own decision-making bodies, sometimes making different and even contradictory policies.



Sectoral policies

"The need for integrating national ICT strategies overlaps with four well-established policy fields: technology, industry, telecommunications and media. Sectoral policies such as education, employment, health, welfare, etc, are increasingly having to address issues relating to ICTs and the growing interdependence between the development of ICT policies and sectoral policies. Experience to date has shown that, in the absence of an existing national ICT policy, the tendency is towards the creation of sector-dependent policy that addresses only its own ICT needs. These policies become firmly entrenched within the sector and later attempts to integrate them into a broad all-encompassing ICT policy become difficult."



Source: R Mansell and U When, 1998, cited in *Information Policy Handbook for Southern Africa*, Chapter 1 http://www.apc.org/books/ictpolsa/ch1/ch1-1.htm

Although policies are formally put in place by governments, different stakeholders and in particular the private sector make inputs into the policy process and affect its outcomes. Thus, for example, in the International Telecommunications Union, an intergovernmental body for governments to coordinate rules and regulations in the field of telecommunications, the influence of multinationals has grown enormously. Privatisation of state-owned companies has meant that governments can rarely control telecommunications directly. The privatised telecom companies, often partly controlled by foreign shareholders, look after their own interests. In the context of globalised markets, large and rich corporations are often more powerful than developing countries' governments, allowing them to shape the policy-making process.

Two sets of issues in ICT policy are critical to civil society at the moment: access and civil liberties. Access has to do with making it possible for everyone to use the internet and other media. In countries where only a minority have telephones, ensuring affordable access to the internet is a huge challenge. Much of the response would lie in social solutions such as community or public access centres. In richer countries, basic access to internet is available almost to all, and faster broadband connections are fairly widespread. Access to traditional media is now a key concern, as new technologies make community video, radio and television more feasible than before.

The other set of issues, civil liberties, includes human rights such as freedom of expression, the right to privacy, the right to communicate, intellectual property rights, etc. These rights as applied to broadcast media have been threatened in many countries, and now the internet, which began as a space of freedom, is also threatened by government legislation and emerging restrictions. Some of the most blatant attacks on freedom of expression come from developing countries such as China and Vietnam, but even in countries which have a long tradition of freedom of expression, such as the USA, there are new attempts to restrict internet users' privacy and to limit their right to choose. At the same time, restrictions that are intended to limit media monopolies are being weakened and pushed aside.

Some examples of recent government ICT policy legislation

- Millennium Act (USA)
- RIP Act 2000 (UK)
- EU Copyright and Patenting Directives
- The Internet Content Filtering Ordinance (South Korea)
- The Council of Ministers Resolution of February 12, 2001, rules for internet use (Saudi Arabia)

Sources: http://www.arl.org/info/frn/copy/dmca.html; www.hmso.gov.uk/acts/acts2000/20000023.htm; http://www.efa.org.au/Issues/Censor/cens3.html#sk; http://www.al-bab.com/media/docs/saudi.htm

Policy is also influenced or even decided by companies and institutions

When Mexico was considering adopting free software in its education system, Microsoft offered money and free licences to the government, which eventually dropped GNU/Linux and embraced Windows completely.

According to the Wall Street Journal, a group of companies and industry organisations undertook a campaign to stifle Internet-privacy legislation. Led by the Online Privacy Alliance (http://www.privacyalliance.org/) in Washington, the loosely organised campaign attacked legislative proposals on three fronts: identifying expensive regulatory burdens, raising questions about how any US internet law would apply to non-internet industries, and assuring lawmakers that privacy is best guarded by new technology, not new laws. Members of the Online Privacy Alliance include Microsoft Corp (MSFT), AOL Time Warner Inc (AOL), International Business Machines Corp (IBM), AT&T Corp (T), BellSouth Corp (BLS), Sun Microsystems Inc (SUNW), the Motion Picture Association of America and the United States Chamber of Commerce.

Sources: http://www.eff.org/Net_info/Tools/Ratings_filters_labelling/; http://www.infoworld.com/article/02/06/12/020612hnemexico_1.html; http://www.privacydigest.com/2001/03/13

The courts also decide policy

The music industry has won at least 871 federal subpoenas against computer users suspected of illegally sharing music files on the Internet, with roughly 75 new subpoenas being approved each day, U.S. court officials said Friday. The effort represents early steps in the music industry's contentious plan to file civil lawsuits aimed at crippling online piracy. Subpoenas reviewed by The Associated Press show the industry compelling some of the largest Internet providers, such as Verizon Communications Inc. and Comcast Cable Communications Inc., and some universities to identify names and mailing addresses for users on their networks known online by nicknames such as "fox3j," "soccerdog33," "clover77" or "indepunk74." The Recording Industry Association of America has said it expects to file at least several hundred lawsuits seeking financial damages within the next eight weeks. U.S. copyright laws allow for damages of $750 to $150,000 for each song offered illegally on a person's computer, but the RIAA has said it would be open to settlement proposals from defendants.

The campaign comes just weeks after U.S. appeals court rulings requiring Internet providers to readily identify subscribers suspected of illegally sharing music and movie files. The 1998 Digital Millennium Copyright Act permits music companies to force Internet providers to turn over the names of suspected music pirates upon subpoena from any U.S. District Court clerk's office, without a judge's signature required.

"http://clearstatic.org:2396/user/view/1"

Source: Fox News, http://www.foxnews.com/story/0,2933,92351,00.html

1.3. Involvement in ICT policy

Why should we, as citizens, become involved in ICT policy-making? The obvious answer is that, as shown above, ICTs are so central to contemporary society that they affect us continually in many ways. So, for example, if a government decides to promote free software, we are more likely to enjoy the benefits of free software (better security, lower cost, easy adaptation to local conditions and needs, etc). This is because it will be more extended throughout society, the monopoly of Microsoft software and its file formats will be broken, and our lives will improve. If a government decides to introduce a new form of censorship on the internet, or fails to protect citizens' rights to privacy, then we will suffer too. If the telephone companies keep prices artificially high for broadband, or refuse to introduce a cheap flat rate for modem access, then we may have to pay too much to access the internet, the same as everyone else. If telecommunications companies are not encouraged or obliged by regulation to roll out services in rural areas, people there will have to rely on more expensive mobile phone services. If governments do not make it legal for wireless internet services to operate, development and community workers in 'unconnected' parts of the world will not be able to benefit from the power of online communication and information access. The internet makes it possible for local voices to be heard throughout the world but, if policy and regulation limit their access, they will also limit their reach.

These self-interested reasons are not the main ones. Other reasons have to do with the nature of global society. If we want to promote social justice, then ICT policy will be a key factor in this battle, and we cannot afford to remain outside the ICT policy-making process.

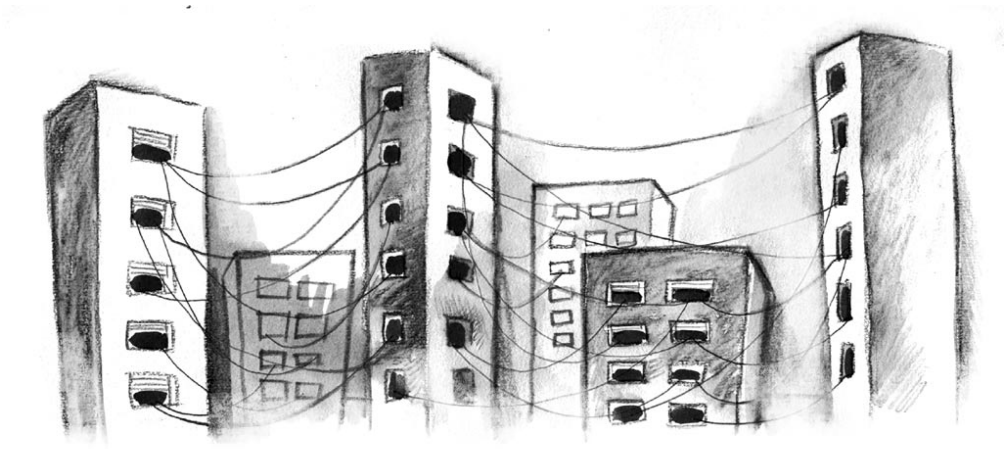
A globalised world and networking

Globalisation is a historical reality, not just a catch phrase. The world we live in has changed enormously in the last 15 to 20 years. While a global economy has existed for centuries, in the form of colonialism and world trade, a new form of unregulated expansion has taken shape in the last decade. The basis of the new economy has been free trade, unrestricted investment, deregulation, balanced budgets, low inflation and privatisation of state-owned enterprises and infrastructures. At the same time, restrictions on financial markets were lifted. A large number of mergers and company takeovers mean that many industries have become dominated by a few multinationals, while smaller, local companies have gone under or been forced to depend on the larger ones.

ICTs have been a fundamental part of this process. Without instantaneous, global, electronic telecommunications, the world financial market could not exist, nor could companies coordinate their production strategies on a global level. Today's competition between companies depends on such global communications, as does the production of new ideas and research, whether at universities, private institutes or company laboratories. Although it is not true to say that ICTs have caused these radical changes, they have been a prerequisite and are now fundamental to the functioning of the global economy.

Manuel Castells, in his three-volume work on the information age[1], has suggested that this modern, globalised, deregulated and privatised form of capitalism is not only based on modern ICTs, but on the forms of social organisation that these permit: networks. A networked society is one in which "the entire planet is organised around telecommunicated networks of computers at the heart of information systems and communication processes."[2] This dependence on the power of information reaches us all. Furthermore, "the availability and use of information and communication technologies are a prerequisite for economic and social development in our world. They are the functional equivalent of electricity in the industrial era." Castells goes so far as to state that ICTs can allow countries to "leapfrog stages of economic growth by being able to modernise their production systems and increase their competitiveness faster than in the past."[3] Whether or not one shares his optimism for the possibility of ICTs furthering social development, he develops a compelling case that this modern economic and social system is not only the most productive one ever but also the most exclusionary. What, and who, it does not need, it casts aside. If you are not part of the networking system, then you are excluded and forced to survive on the outskirts of it, marginalised, powerless and poor. While the powerful use networks to go beyond the traditional restrictions of space and time, most people all over the world cannot. People, workers, citizens, do not function on a day-to-day level in a global network, but at a local level in a closer human web of human relationships.

The conclusion is clear: we have to use the networks in a new way, for the benefit of human beings and not for the efficient functioning of the international money market and multinational companies.[4] If global, networked systems are the new basis of power, and if ICTs are the technical foundation of globalisation, they became a terrain of struggle. The main challenge is to adapt them to become the technical foundation of the struggle against the negative impacts of globalisation and for social justice. Those who remain inside the networked society, with access to the systems that make it function so effectively, will be able to fight to change it. Those who are excluded will find it so much more difficult.



1 M. Castells, *The Rise of the Network Society*, *End of Millennium* and *The Power of Identity*, 1996-2000.

2 *Information Technology, Globalization and Social Development*, 1999, http://www.unrisd.org/unrisd/website/document.nsf/F270E0C066F3DE7780256B67005B728C?OpenDocument

3 Ibid.

4 This argument is explained at length in *The Rise of the Network Society* (2000), where Castells develops his notion of the 'space of flows', as distinct from the traditional 'space of places'.

Yoshio Utsumi, Secretary-General of the International Telecommunication Union (co-organiser of the WSIS), in an address to the UN General Assembly, New York, 17-18 June, 2002:

"Of course people cannot live on information alone, but it is quite obvious that humanity, for better or worse, is now entering an age where information-oriented activities are a major part of GDP (national income). Information is a key to competitive advantage both for businesses and modern states. Therefore, it becomes all the more urgent to build the basic telecommunication infrastructure, to develop capable human resources and to make the best use of information technologies for every aspect of human activity. We must extend the benefits of information and telecommunication technologies to every citizen in the world. We must bridge the digital divide and turn it into a digital opportunity."

Source: http://www.rthk.org.hk/mediadigest/20020715_76_33709.html

So what should we do with the new technologies?

What does this mean in practice? It means using ICTs to do several things. First, to spread alternative information in a new way, to millions of people instantly and without the confines of traditional limitations such as distance. Second, to create new forms of organisation and coordination, new structures and new modes of operation. Third, to foster new forms of solidarity among the powerless, new ways of sharing experience and of learning from one another. And finally, to incorporate more and more people into these alternative global networks.

People are already doing it. The Web allows anybody to publish news and information, and the effects of this can be seen everywhere, not just on the millions of websites that anyone can access. No longer can the powerful tell lies and get away with it so easily. For example, when a politician justifies a war with lies, alternative versions immediately appear on thousands of electronic mailing lists, websites, blogs, and internet radio and TV. Websites like the Indymedias provide alternative sources of information, which are instantaneous, open to the participation of anyone who has interesting news, and where information, opinion and debate coexist. Information can now be made available instantly all over the Web. This forces the traditional media, such as the mainstream press and TV, to respond, changing the style of information gathering but showing, as they compete for momentary exclusives and news-breaking stories, that their news and information are still controlled by the editors, the directors, and frequently the owners. Counter information on the internet is usually unpaid, and allows other viewpoints to be heard.

But it is not only the information flows that are changing. The way we work together is also changing. New tools allow new ways of organising, often without the vertical hierarchies, rigidly formal structures and entrenched office bearers that previously allowed those who controlled the information flows to control the structures. A mailing list makes it just as easy to send a message to hundreds or even thousands of people as to one person. When activities are organised through a list, everyone can have all the information, not just chosen bits. Thus a coalition of activists can be not just a few representatives who go to a meeting once a week, but hundreds of people who can voice their ideas. A campaign for mass demonstrations, or to protest a political trial, can quickly involve thousands of people in a matter of weeks, when previously it would have taken months or years. This makes grassroots-organising easier, allows more people to be involved, but also may mean that the political structures that are developed in this manner are not so stable as they used to be. A network may develop for a particular campaign, involve a dozen, hundreds or thousands of people, and then dissolve or change into another form when the campaign finishes.

A unionist comments on the use of email

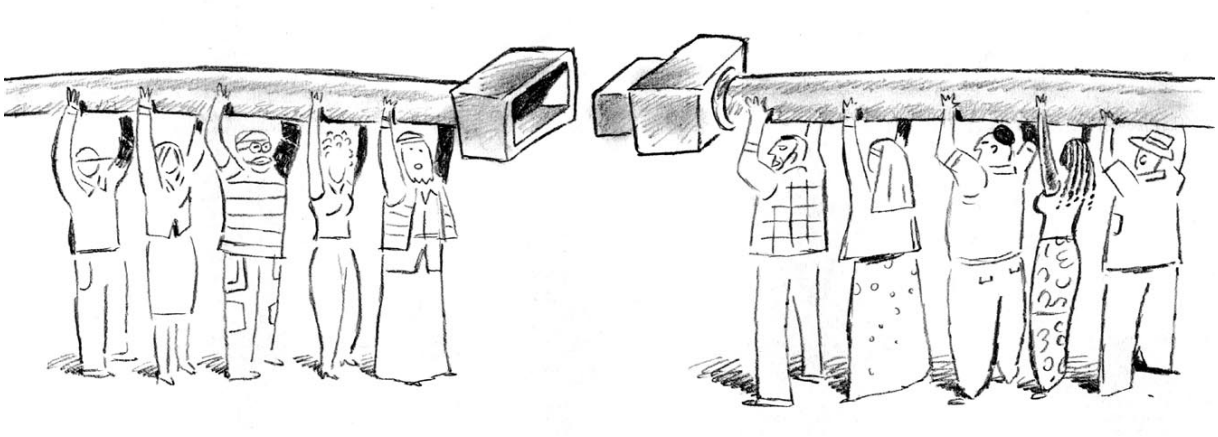
"Before, when information arrived by fax to the local union office, I never knew what was going on. If I made the effort to go into the office, the fax might be on the notice board, but half the time it had fallen off and been put into the bin, or someone had taken it home, etc. Then we started using email in the office and the first thing I used to do when I arrived was look in the computer to see the new emails. Now that we are all on the Net, I have a copy of everything that reaches the local office. I can comment on it through the list and we can discuss things before the meetings, which makes them quicker and less boring. Now I get too much information, quite the opposite from before.

Source: Personal communication

One challenge faced by those working for social justice in the era of globalisation is how to operate on a global scale, to link people and communities in different countries around causes that affect us all. Apart from email and mailing lists, web forums, news groups, intranets, online group work spaces, webs, blogs, videoconferences, instant messenger services, and a host of new tools mean that the possibilities for international, national or local collaboration are infinitely greater with the new technologies. In the same way that injustice has become globally organised, the struggle against it must be global, not only local. This means that people from rich countries can learn from those from poorer countries, and vice versa. Of course, ICTs are no substitute for real, face-to-face interaction, but when this is not possible they can provide alternatives. And they often make closer human communication easier by bringing people together.

But to use the new ICTs in these ways, you need to be able to access them, and most of humanity cannot do so at the moment. Access to ICTs for all is thus a key demand for concerned citizens, an essential aspect of ICT policy, and an issue for us all.

The new technologies offer enormous possibilities for increasing human freedom and social justice. The origin of the internet, designed as a way of collaborating without any central control, makes it an excellent tool for this, and because the internet has developed in an unregulated way on the basis of collaboration, it is not controlled. Not yet. But this situation is unlikely to last. In fact, it is under threat from governments and multinational companies, through legislation, regulation, monopoly control, legal pressures, and intellectual property restrictions. The new ICTs will not be new for very long, and they might not continue to be as free as they are now. The possibilities they offer can be taken away from us, unless we actively participate in the inevitable regulatory process that any new technology experiences.



Examples of global campaigns using ICTs

The international campaign to ban the use of land mines is a pioneering example of the use of the internet to reach a world-wide audience and bring together various NGOs in a coalition. It culminated in 1997 in an international agreement not to use these weapons.

Source: http://www.icbl.org/lm/1999/; http://www.globalpolicy.org/ngos/governance/landmines/0925bangkok.htm

Since 1996, Amnesty International has mounted campaigns around human rights in Nigeria which put enormous pressure on the Nigerian dictatorship. Recently these campaigns have included saving the lives of women sentenced to death by stoning under Islamic law. Email petitions have been widely distributed.

Source: http://www.amnesty.org/ailib/intcam/nigeria/; http://www.cnn.com/2002/WORLD/africa/06/05/nigeria.amnesty/

Act now, before it is too late

Now is the time to act, when all is not yet decided. If we wait until the restrictions on ICTs are consolidated, it will be much more difficult to reverse policies than to create better ones in the first place. Policy varies from country to country, especially from rich to poor, and the priorities are different. In poorer countries, where ICTs are less developed, the key issues are access to ICTs for the majority of the population and outright restrictions such as internet filters and lack of freedom of expression. In the developed countries, many of these issues have already been decided, such as telephone access, or have a long tradition, such as the lack of censorship. But new issues are arising as restrictions are imposed: privacy, censorship, intellectual property restrictions, broadband, 3G cell phones, wireless connectivity, infrastructure monopolies, media concentration, etc. The result of these new struggles to impose the power of governments and multinationals will inevitably

be extended to the rest of the world, so people in less developed countries should actively engage with these issues, because their future will be decided for them.

So why should we be interested in ICT policy? Because the way ICTs develop will have an enormous impact on the possibilities of working for social justice and sustainable development. If we do not take an active part in ICT policy-making, we will have no say in how our societies develop and how the future unfolds.

Wireless

The use of wireless to connect to the Internet is another rapidly expanding Information and Communication Technology. It is another example of an area of freedom, not yet fully regulated, which could become more controlled. Already the US Defence Department is complaining that the 809.11 protocols use bandwidth that the military needs. Lawrence Lessig argues that wireless should be available to everyone, and that users will lose out if it is controlled, sold off, restricted and regulated.

"Wi-Fi is the first successful example of these spectrum-sharing technologies. Within thin slices of the spectrum bands, the government has permitted "unlicensed" spectrum use. The 802.11 family of protocols has jumped on these slivers to deliver surprisingly robust data services. These protocols rely on a hobbled version of spread-spectrum technology. Even in this crude implementation, the technology is exploding like wildfire.

And this is just the beginning. If the Federal Communications Commission frees more spectrum to such experimentation, there is no end to wireless technologies' potential. Especially at a time when broadband competition has all but stalled, using the commons of a spectrum to invite new competitors is a strategy that looks increasingly appealing to policy makers."

Source: L Lessig, *Wireless Spectrum: Defining the 'Commons' in Cyberspace*, http://www.cioinsight.com/article2/0,3959,1151656,00.asp

The internet, markets and access / part 2

The internet, markets and access

There is a range of issues involved in 'democratising' the internet, but we must begin with the question of how to 'enfranchise' internet users by making access more equitable and affordable. In developed countries, users have often complained about the high cost of internet access, as in the internet strikes in Europe in 1998-99, where many users in Belgium, France, Italy, Poland, Portugal, Spain and Switzerland refused to connect for 24 hours to protest the high cost and to demand a low flat rate. The paradox of the digital divide is that it is often more expensive to access the internet in developing countries than it is in developed countries.

For example, an individual user in the USA accessing the internet over an ADSL line at 512 Kbps has the same bandwidth as the entire country of Sierra Leone. The monthly cost of this bandwidth is around US$50 in the USA, but in Sierra Leone it could reach US$4,700. At each step of the way it is more expensive to access the internet in the developing world than in the developed world. This is because of the telecommunications infrastructure on which access relies, and the governance structure of the internet. As with any commodity, volume affects price. Developing countries with less internet traffic than developed countries will find it harder to obtain cheaper prices.

In this Part 2, we look at some of these inequalities, with particular reference to Africa – where the problem is most acute – explain how they come about, and provide some pointers regarding access for all people in developing countries. This involves analysing how the costs of the internet are shaped, partly by its unique technical structure (chapters 2 and 5) but also by its commercial set-up (chapters 3 and 4). Some regional differences are explained in chapter 6, and chapter 7 then looks at how the technical infrastructure affects internet governance. Finally we look at some initiatives to address the problems raised in this part of the book.

2. Internet Basics

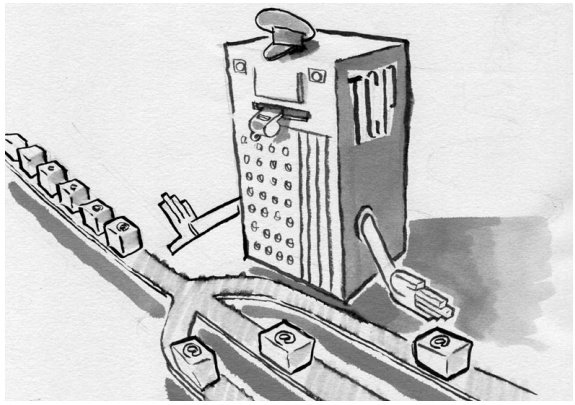
When most people think of the internet, they think of a computer screen with pretty text and images – the familiar World Wide Web page. But the internet is not the same as a web page. It pre-dates the Web, and has many other functions such as email, news groups, videoconferences, chats, voice over IP, p2p networks (none of which are web-based), and the list is getting bigger.

How has the internet developed?

The internet began in the USA during the Cold War. When the Soviet Union placed the Sputnik satellite into space in 1957, the US military was shocked, which led to the creation of the Advanced Research Projects Agency (ARPA). One of ARPA's projects was to investigate large-scale networking of computers, especially to allow collaboration between scientists and researchers. It was to be a decentralised network, without a central focus or control point, so that if one node in the network failed, the others could take over its role. The decentralised nature of the intetrnet is said to have been inspired by the idea of surviving a nuclear attack. A centralised communication system could be put out of action easily with a missile, but if all the points on the network could replace the destroyed node, if none was essential to the functioning of the network as a whole, then the system would be able to withstand at least limited damage. In fact, the initial motivation was more how to avoid centralised control, and the need to stimulate cooperation amongst researchers. And it was to be open to connection with other systems via publicly available standards.

In 1969, ARPA scientists connected two (and soon thereafter, four) mainframe computers (there were no PCs then) in different states of the USA, and began to send data to each other via a rudimentary packet system, the beginnings of the internet protocols that we use now.

Thus ARPANET was born, and was presented to the public in 1972. By then, simple email was possible, computer-to-computer chats followed, and other countries began their own research networks. In 1979, USENET brought us news groups, but at that stage only a few hundred computers were involved. Of course, the Web still did not exist, everything was text-based and, although other networks were created in the USA, Canada and Europe, which were similar to ARPANET, they still were not all interconnected.



The first internet trials

The idea was to type 'login' at UCLA and see if this appeared on the other computer at Stanford University.

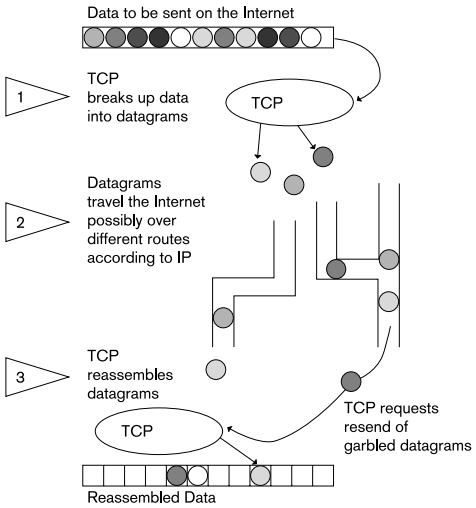
"We set up a telephone connection between us and the guys at SRI," Kleinrock said in an interview. "We typed the L and we asked on the phone,

"Do you see the L?"
Yes, we see the L," came the response.
We typed the O, and we asked, "Do you see the O?"
Yes, we see the O.
Then we typed the G, and the system crashed…

Yet a revolution had begun"…

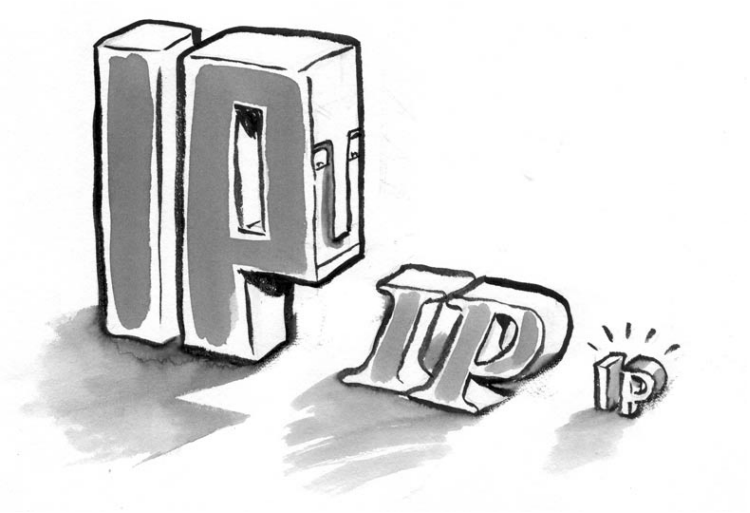
Source: Sacramento Bee, May 1, 1996, p.D1, cited in *The Roads and Crossroads of Internet History* by Gregory Gromov, http://www.netvalley.com/intval1.html

But what they were beginning to share was the fundamental basis of the internet, the TCP and IP protocols. Formally adopted in 1982, these technical standards allow the internet to function as a decentralised network of interconnected computers. The TCP protocol defines the way data is broken down into manageable chunks, or packets, which are then sent individually through the internet. Imagine a large letter is broken up into separate pages. Each page is put into its own envelope and then into the post box. When they reach their common destination, they are put back together to create the original file or piece of data. This is more efficient than, for example, a continuous flow of data, because if one of the packages is lost, it can be re-requested and sent without having to re-send all the data, causing less errors and less wasted time.



Source: http://www.asc.upenn.edu/usr/chunter/agora_uses/chapter_2.html

The IP protocol controls the way the packets reach their destination, a kind of addressing system based on IP numbers such as 123.123.123.123. It is a bit like the address on an envelope. Each computer on the route to the destination knows how to send the packet to its IP destination, choosing the best route according to which computers are available and connected at each point in time. There is no direct connection between the origin and the destination, and the route is not decided in advance before the journey begins. Routers decide where to send the packets, depending on which other hosts are available, and the packets jump from one host to another until they finally reach their destination. To be on the internet, you need an IP number, as well as a physical connection such as a phone line, an Ethernet or cable connection. In theory, no IP number is more important than another – the internet has no central brain or headquarters. In practice, as we will see, some IP numbers, such as those assigned to the DNS databases, routers and backbone nodes, are more important than others.



This system is different from the traditional information flow used in the telephone system, called circuit switching. Here, the flow of information is continuous, along one channel. If this circuit is broken, the connection is lost and communication stops. In packet switching, in contrast, if the flow is stopped for some reason, the routers are able to find alternative routes, and not all packets need to follow the same routes as each other, before they are brought together and reassembled at their destination.

By 1984, the number of IPs was around a thousand, and it was impossible to remember them all, so the Domain Name System (DNS) was introduced. This meant that an internet address could be made up of words, not just numbers. When you typed in the address, whether in email, or a news group (remember, at that stage there was still no WWW or hypertext), your programme asked a central database for the IP number that corresponded to that name, and used that IP number to send the packets to their destination. For a name to work it had to be registered first; otherwise it would not be in the database. All internet name addresses (as distinct from IP addresses) must use a domain. The first domains were .mil, .edu, .com, .org, and country domains such as .uk were introduced from 1985. That same year, the task of running the DNS database was given to the Information Sciences Institute (ISI) at University of Southern California (USC), and domain name registration was run by the Stanford Research Institute (SRI). The internet was still very much a network for researchers, and the organisations that ran it were university-based. In 1986, the National Science Foundation set up NFSNet, which provided a backbone of fast fibre optic connections to which other centres in the USA, mostly universities, could connect easily. The Internet Engineering Task Force was set up the same year to decide on the technical standards for the entire internet also with a little US university funding. This means that the US government essentially paid for the physical infrastructure and the running of the entire network, with the exception of those networks in other

countries which were beginning to connect up to the US network, and which were research networks funded in turn by their own governments. There was still no commercial internet, and almost all users were from universities or research institutes. It was not until 1993 that the introduction of the graphical World Wide Web made it much easier to present and find information on the internet. Together with the commercial exploitation of the internet, which took off around 1994, this created the expansion boom that has led to the millions of users we have now.

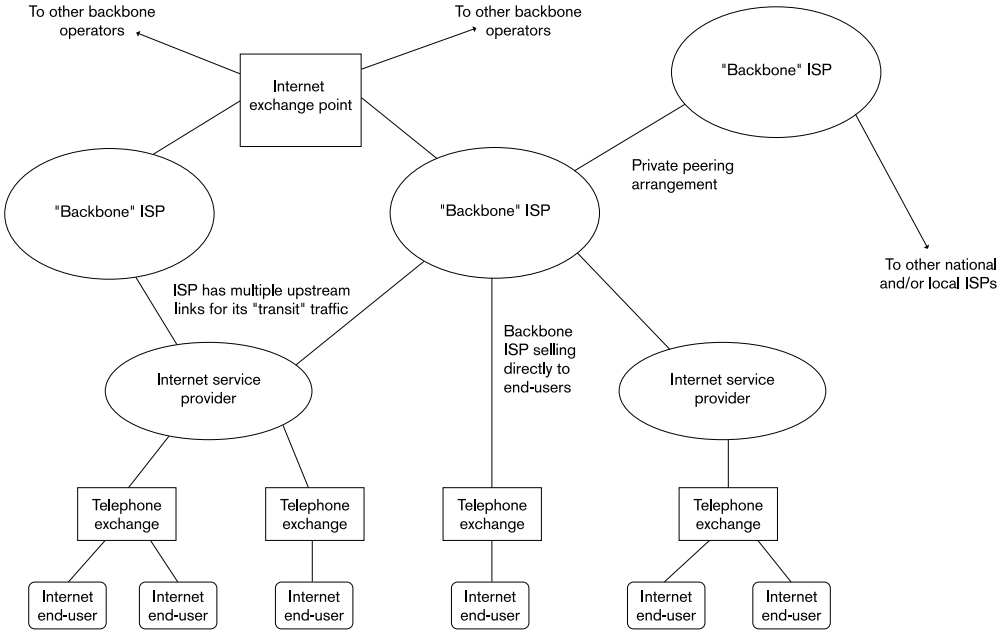
Internet Structure

How does the internet work now? The underlying basis is the same: a whole lot of computers connected up to transfer data from one to the other. Data can flow through fibre optic cables, copper wires, coaxial cables, copper telephone lines, satellite connections, wireless, Ethernet cables, etc. It still uses the TCP/IP protocol that moves the data from place to place. On top of this, there are various other protocols that allow us to do useful things with the data. For example, the SMTP protocol sends email on its way to another internet server. It is not necessary to use the SMTP server on your own ISP system, although most systems are protected from external spammers so that only that ISP's users can access the data. The HTTP protocol allows your web browser to send a request for one or more web files to another computer (web server). When the text and graphics files reach your browser, it interprets the HTML language in the text files, laces the graphics and the colour in the appropriate place, and assembles them all to create the visually-pleasing page you see on your screen. The POP protocol allows us to login to a POP server and download our mail to be stored on our own computer, rather than only view it on a web page while we are connected to the internet. IMAP allows many other kinds of files and applications, such as audio and video, to function together via the web.

To connect to the internet, you can be on a local network which is connected already, as in a library or university, or have a special cable which connects you directly, such as a leased line (a special cable leased from the telecommunications company which provides fast but expensive access) or a cable TV connection, or have a contract with a company which provides a satellite connection, or through a local wireless connection point. Most people however, connect via the telephone system with a modem or ADSL, using their telephone wire (via the 'local loop' between the telephone and the telephone exchange) because it is cheaper and more readily available. In general, the faster the connection, the more it costs.

When you connect via a commercial link, it is normal to do that through a company or Internet Service Provider (ISP), which has a permanent connection to the internet and charges you for sharing this connection with hundreds or thousands of other users. The ISP only routes local traffic to a commercial carrier, usually a telecommunications company or a huge ISP, with a further connection to the main highways of the internet, which most people never see. The first of these backbone carriers was NFSNet, back in 1986, but now huge companies, such as UUNet, Sprint, and ATT, run the most important internet infrastructure. They connect to each other through Major Exchange Points (MAPs, MAEs, etc) and in this way the internet extends over the face of the planet. So we have:

1. End users
2. ISPs
3. Carriers
4. Major Exchange Points
5. Backbone carriers



Most of this infrastructure is owned and managed by private enterprise, rather than by governments, and hardly ever by community organisations. This early privatisation has had important consequences for the subsequent development of the internet, and this is explored in more detail in chapters 3 and 4.

The World Wide Web

The early internet had no graphics. Everything was in text form: letters, numbers and symbols on the screen. The introduction of the World Wide Web ('the Web') revolutionised the internet, making it more attractive, more versatile and easier to use. The Web was initially conceptualised by Tim Berners-Lee and other scientists at the European Centre for High Energy Physics (CERN) in Geneva, Switzerland in 1989, and a simple – and free – browser was released to the public a year later. Initially progress was slow, with no more than 150 web sites in the world by the end of 1993. It was the creation of the Mosaic browser programme by Mark Andreeson in 1993 that simplified enormously the use of the Web and made the pages so easy to read and visually pleasing. This was the predecessor of Netscape and Microsoft Explorer. The programme was made available to the public, especially to the educational community, and it rapidly replaced the text-based tools for information retrieval like Gopher, Archie and Veronica that had been used before. In 1994, the WWW edged out telnet to become the second most popular service on the Net (behind ftp-data) based on the percent of packets and bytes traffic distribution on NSFNET, and a year later it became – and has remained – number one.

It was in 1994 that private enterprise started using the internet, with the commercial sites and the first virtual shopping malls and cyberbanks. In 1995, NFSNet became a research network again, and the infrastructure was now firmly in the hands of private enterprise. The internet began to be sold as a commodity, and it sold well. In 1994, there were 3,000 web sites and a year later 25,000.

There are many problems with this way of financing internet infrastructure. To begin with, monopolies in the telecommunications industry can mean that prices are artificially high and competition is minimal. The USA dominates the internet, both in terms of number of users and amount of content. Economies of scale mean that it is cheaper to connect to the internet in the USA than in other parts of the world, since the infrastructure there is better developed and US companies control it worldwide. And, because of the way ISPs are charged for their connectivity, it is more expensive for ISPs in poor countries than in rich ones. Coupled with higher fees for telephones, the result is that users in poor countries have to pay much higher prices than those who can afford to pay more. This means that very few can benefit from the advantages of the internet in those countries. Internet infrastructure used to be horizontally organised, but now, with the dominance of huge multinationals, it is much more vertically organised.[1]

The inventor of the web talks about the internet:

"The Internet ('Net) is a network of networks. Basically it is made from computers and cables. What Vint Cerf and Bob Khan did was to figure out how this could be used to send around little "packets" of information. As Vint points out, a packet is a bit like a postcard with a simple address on it. If you put the right address on a packet, and give it to any computer which is connected as part of the Net, each computer would figure out which cable to send it down next so that it would get to its destination. That's what the Internet does. It delivers packets - anywhere in the world, normally well under a second.

Lots of different sort of programs use the Internet: electronic mail, for example, was around long before the global hypertext system I invented and called the World Wide Web ('Web). Now, videoconferencing and streamed audio channels are among other things which, like the Web, encode information in different ways and use different languages between computers ("protocols") to provide a service.

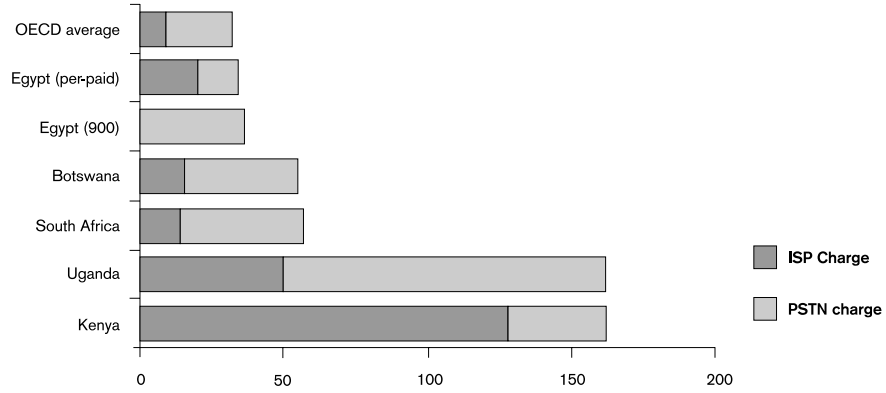
The Web is an abstract (imaginary) space of information. On the Net, you find computers – on the Web, you find document, sounds, videos,.... information. On the Net, the connections are cables between computers; on the Web, connections are hypertext links. The Web exists because of programs which communicate between computers on the Net. The Web could not be without the Net. The Web made the net useful because people are really interested in information (not to mention knowledge and wisdom!) and don't really want to have know about computers and cables."

Source: http://www.w3.org/People/Berners-Lee/FAQ.html#General

1 P Dogan, "Vertical Relations and Connectivity in the Internet", in *Communications and Strategies*, 47, 2002, pp. 87-101

Internet price comparisons (US$)

Based on 20 hours, off-peak use per month



Source: http://www.itu.int/africaInternet2000/Documents/ppt/Tim_Kelly_2nd.ppt

3. Internet Economics: What things cost (in different countries) and who pays

User costs – 'free' to the user but who pays?

The internet appears 'free' to the user. If you are using a dial-up account, once you have paid for a telephone connection to an ISP and the subscription costs of the account, browsing the internet or transferring emails is essentially free. But the internet has never been free in the monetary sense. In the beginning, the US government paid for the infrastructure, first via its military research programme (ARPA), then through the universities (NFSNet, etc). Now, internet is big business, and someone has to pay for everything. The ordinary user pays the ISP to be connected. The ISP may charge a monthly flat rate, or according to the amount of data that the customer receives/sends, or the number of hours connected. The ISP in turn has to pay the telecommunications company or another ISP for its connection to the internet, and perhaps for the rental of computers or other services, apart from its normal running costs. The customer also has to pay for the telephone line, with a monthly rental and a fee for each (normally local) connection. Many telephone companies charge by the minute for local calls so the longer the user is connected the more expensive the connection. In fact, even when some ISPs offer 'free' connections to the internet, they usually offer the connection for free, but by arrangement with the telephone company they earn money from the telephone charges for the call.

When accessing a web page or sending an email, the packets are routed through the various interconnected networks of the internet to reach their destination, over links which are paid for by the ISPs. Take the case of browsing a website in Fiji from the UK. The user establishes a connection to the internet by dialling up to an ISP's nearest point of presence (POP). From this point on, the user does not pay anything else. The ISP provides a leased line from that POP to its central node, and then to other ISPs where it exchanges traffic with that network, which in turn does so with another network, and so on. The packet is routed through the network of networks until it reaches its destination. The ISP pays the telecommunications company or a larger ISP for its connection, and they in turn pay a larger carrier. The larger companies enter a variety of commercial agreements among themselves, to share the huge number of cables, routers, and computers that make up the global internet infrastructure. In this way, the distance to the website or POP server is not important to the end user, because it does not influence the cost of the communication. We pay for unlimited access to any point on the global network.

The Economic Toolkit for African Policymakers[1], published by the World Bank in 1998, splits the cost of internet access for the user into its component parts. It found that for 30 hours of internet access in Africa, 15% of the cost is accounted for by telephone access, 42% by equipment (37% on computer and 5% on modem), and 43% by ISP subscription. The main upfront cost is computer equipment, which is subject to import tariffs and other taxes in some countries. Equipment costs can be reduced massively by public internet access centres, which lower entry barriers be removing these costs. This is especially so in developing countries where there is a limited number of computers, which naturally therefore limits the number of potential internet users.

Taxes on Computer Equipment

At the international level, countries have entered into World Trade Organisation (WTO) commitments to open markets to trade by lowering import tariffs during the Uruguay round of negotiations. One area of trade is specified under the "basic agreement on telecommunications" and another as "computer and related services". In the first case, countries undertook various standard commitments during the Uruguay round to liberalise their telecommunications sector and allow competition by certain deadlines in different sectors (local, long distance, international, data communications). During the Doha Development Round in 2002, the World IT and Services Alliances (WITSA) campaigned for those countries which have not lowered access in the computer and regulated services to do so[2].

How fast?

Check to see how fast your internet connection is! You can ascertain the speed of your internet connection by double clicking the linked computer icon in the bottom right hand corner of your screen, or by use one of the following websites:

- CNET http://webservices.cnet.com/bandwidth/
- PCPIT K http://www.pcpitstop.com/Internet/Bandwidth.asp
- EIRCOM NET http://homepage.eircom.net/~leslie/testpage.htm

Telephone access costs

The cost of dialling up to the ISP's POP using a telephone line depends on two things: first, the amount of time spent online and second, the tariffs which are charged by the telephone operator. The amount of time which a user needs to spent online depends heavily on the bandwidth of the line. This is measured in the number of kilobits per second, as this determines how long it takes to download a file. Telephone lines are designed to carry voice conversations at 64 Kbps, and modems work at either 56 Kbps or 64 Kbps. In practice, however, speeds are usually much lower than this because of congestion, attenuation of signals, or poor quality analogue lines and switches. Faster lines using ISDN (integrated services digital network) or DSL (digital subscriber line) technologies can be obtained where telephone companies have installed them, or wireless technologies.

1 Africa Internet Forum, UNECA and infoDev project, "Economic Toolkit for African Policymakers", http://www.infodev.org

2 See WITSA http://www.witsa.org, and in particular the "Background Paper on the World Trade Organization's Negotiations and Issues Regarding Information and Communications Technology (ICT)", http://www.witsa.org/papers/WITSA-DohaPaper-final.pdf

The availability of different internet access lines

The availability of different internet access lines is one issue for policy interventions. In the UK for example, action groups have been established in many rural areas to lobby British Telecom to install ADSL in their local exchanges. This pressure can work. By encouraging potential users to register their interest in ADSL, it becomes easier to justify the cost of upgrading the exchange and encourage the company to install the equipment.

For heavy internet users, it frequently becomes more cost efficient to lease a dedicated line from the telephone company and pay a flat price regardless of how much time is spent on the line. Leased lines can be bought at 64 Kbps, 128 Kbps, 256 Kbps, 512 Kbps, 1024 Kbps, 2048 Kbps or above. Organisations or businesses with many computers will connect them together onto an internal local area network (LAN), and then share one 'leased line'. At the point where the costs of dialing-up exceed monthly outlay on a leased line (for example if there are 10 computers which are used for internet access), it becomes more cost effective to lease a line. Where 'broadband' has been deployed (DSL), this is also charged at a flat fee in the same way that leased lines are.

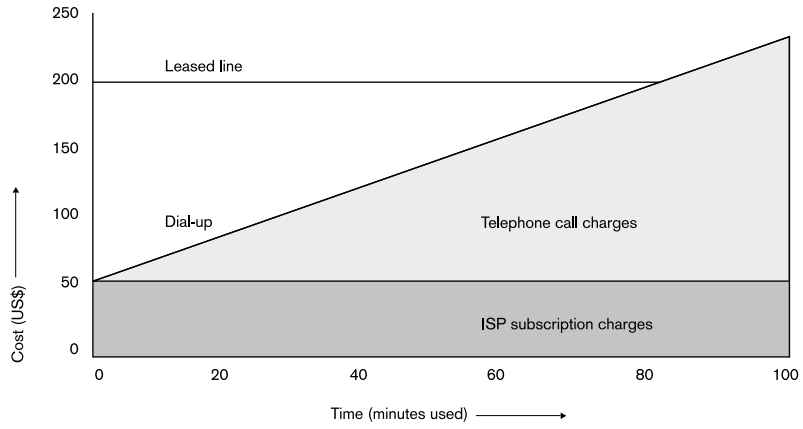
The tariffs charged by the telephone company for lines and leased lines are the key cost factor for internet access, therefore another area of concern for policy makers. These tariffs are set by the telephone company, but in many countries are subject to approval by the regulator. A key lobbying point is for the telephone company to use local rates for dial-up tariffs.

A telecommunications monopoly in a country means that users have no choice of a telephone company to use in order to dial up to their POP, and must accept the tariffs charged. In a competitive environment, users can choose between a number of local exchange carriers, are free to choose the lowest tariff and in so doing lower the cost of internet access. A monopoly over international traffic means that ISPs are not able to establish their own independent links to foreign ISPs and to the internet backbone, and must route all traffic and bandwidth through the telephone company, which can charge whatever price it likes for the international bandwidth.

ISP subscription costs – what the user pays

All the other costs of the internet are hidden from the user. The ISP bears the rest of the upstream costs of the internet, but as a business it must pass these costs back to the end user through the account subscription fees. The ISP subscription fees are usually the highest component of the cost of internet access. Ultimately, unless internet access is subsidised by an organisation (such as a university or a company), the user pays all the costs. ISP subscription fees vary widely, and a number of models have been employed (for example the 'free ISP' model).

Dial-up versus leased line costs for Internet access

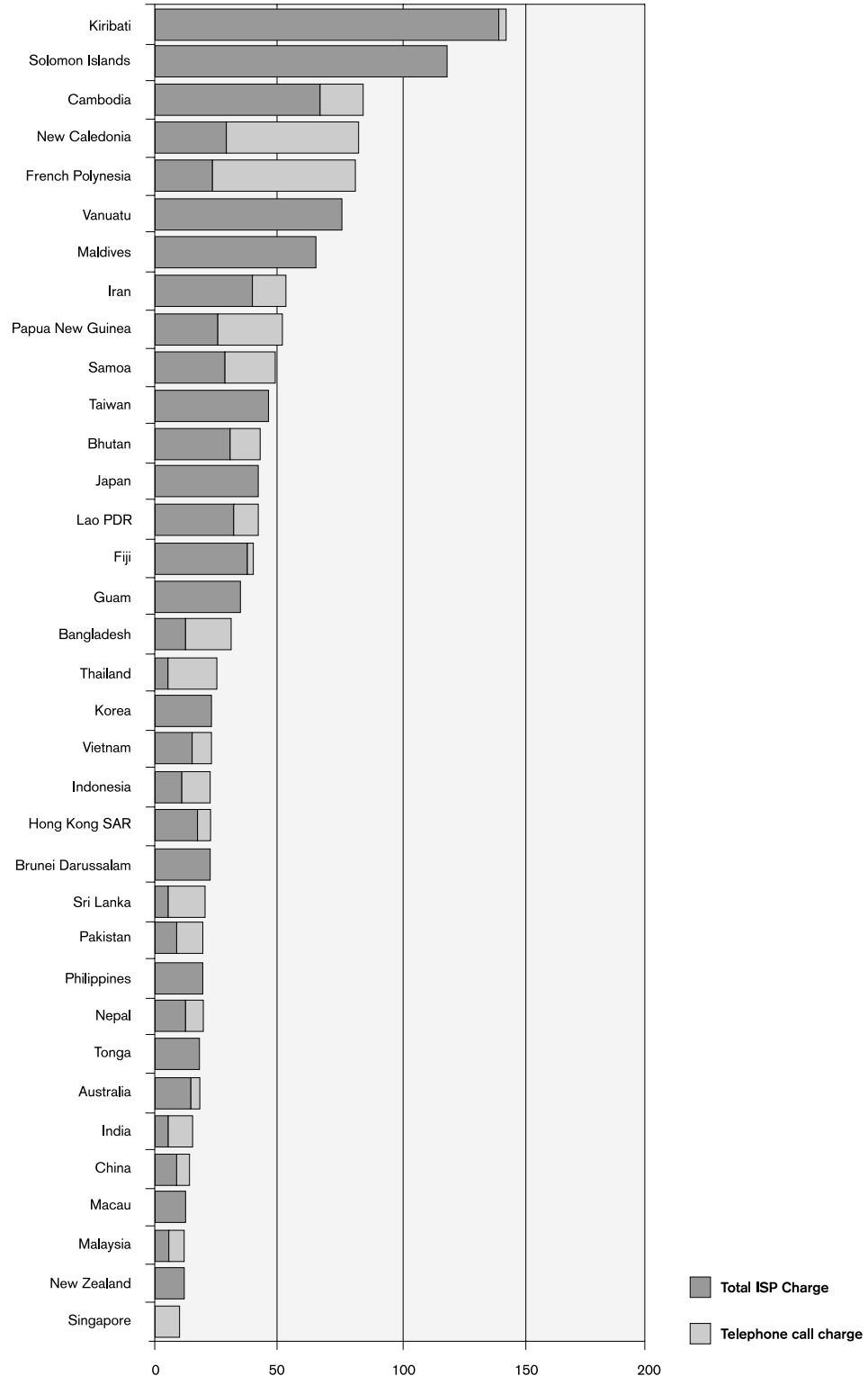


Source: Adapted from ITU

Tariffs can prove more important than the speed of connection for determining access prices. The figure of 15% of the total costs of access, which is spent on telephone calls in the African Toolkit model, is based on local rates. Where users have to make a long-distance phone call to the nearest POP, these costs skyrocket and account on average for 72% of the costs (the rest evenly split between the cost of ISP subscription and the equipment). In the 1990s, before ISPs were established in many countries, to get access to the internet users had to make an international call to dial into the POP of a foreign ISP – which was astronomically expensive.

Using these two variables – telephone charges and the ISP subscription – the cost of internet access varies widely across the world. Most noticeably, the internet

Monthly Dial-up Internet Access Costs (US$), Asia 2002



Source: Asia Pacific Telecommunication Indicators 2002, ITU.

access costs are very much lower in OECD countries than in developing countries. In Asia for example the cost of 30 hours internet access per month in New Zealand is US$11.74 (US$11.74 ISP charges and free local call charges), which is less than a tenth of the cost in Kiribati US$142.8 (US$140 ISP charges plus US$2.8 telephone charges).

ISP costs – what the provider pays

ISPs, which provide the 'on-ramp' onto the internet, are run either as businesses or in the education or government sector. Either way, the ISP bears all the upstream costs of the internet. In the case of commercial ISPs, these costs are passed back to the customer through subscription charges, plus profit. In the public sector, they are run on a not-for-profit basis and may to some extent be subsidised.

Internal network infrastructure: Because of the historic growth of the internet in the USA and OECD countries, leased lines are concentrated in the developed core of the global economy. At the end of 2001, there were around 375,000 permanent leased line connections to the internet around the world, according to Netcraft's leased line survey quoted by OECD[3]. Some 89% of leased line connections to the internet are in OECD countries. The largest number of leased line connections is in the USA with one-third of all connections in the world. Japan makes up 12%, followed by the United Kingdom (7.1%), Germany (6.6%) and Canada (3.3%).

External network infrastructure: The ISP in turn must establish a leased line from a telecommunications company in order to connect to the internet. Again, the cost of leased lines varies greatly between countries, depending on the cost of providing the line and the degree of competition which exists. For this reason, it is economically attractive for ISPs in each tier to connect with each other through formal or informal peering arrangements. Because communication is cheaper locally, and national long-distance is cheaper than international traffic, Tier 3 ISPs would avoid, if possible, sending traffic to a neighbouring ISP through an international link.

Even within OECD countries, "local leased line prices remain of concern where there is currently insufficient competition. For users, in those markets, this means that incumbents can continue to charge prices that are not disciplined by competition." [4]

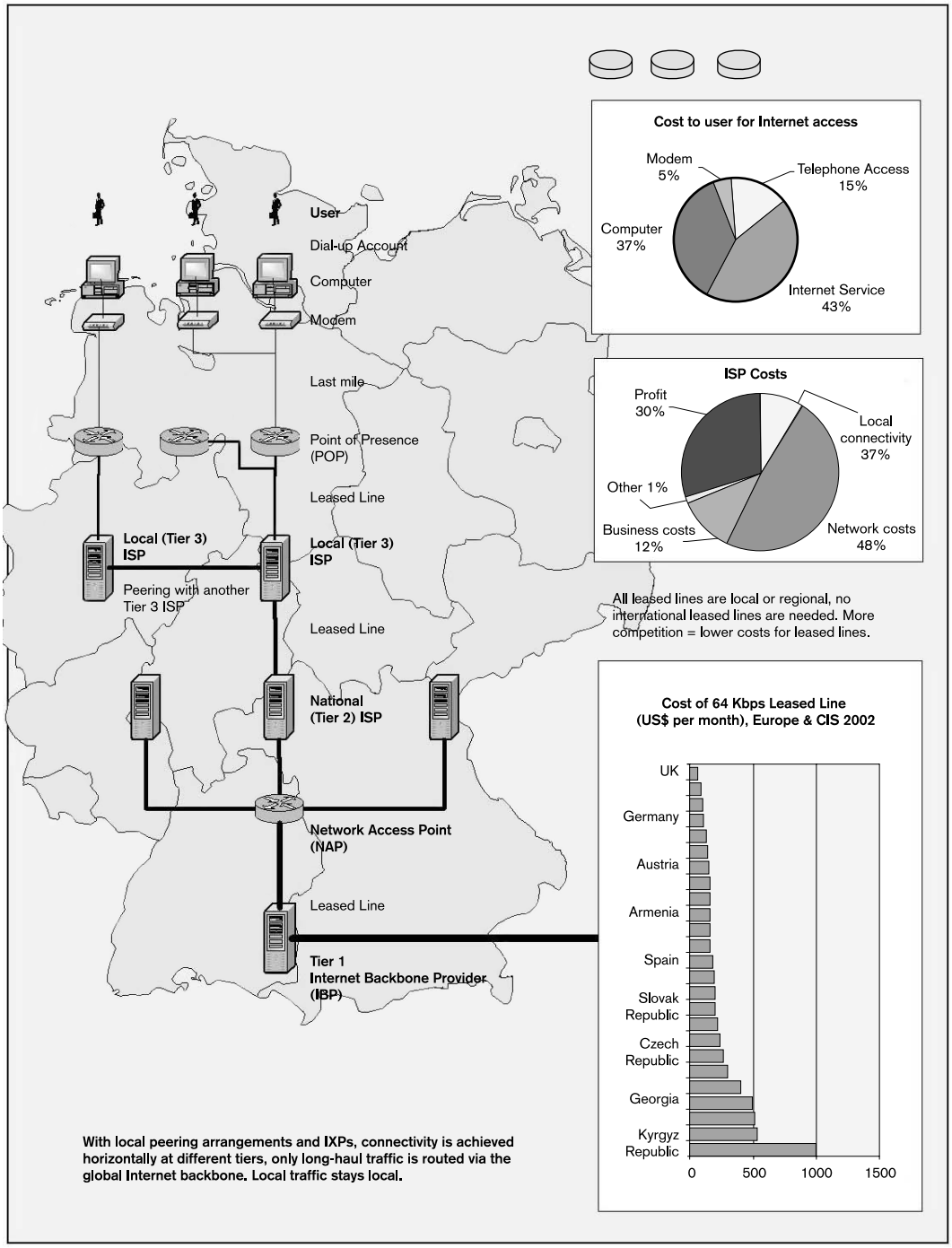
In developed countries such as the USA, upstream service providers are located in the same country as Tier 2 and Tier 3 ISPs, and the telecommunication costs for the latter are lower – they only have to pay local or at most regional leased line rates (plus the transit charge) to gain access to the internet backbone. Furthermore, the generally higher level of competition in developed countries has resulted in lower prices for leased lines.

In many developing countries, where the internet has been introduced relatively late, ISPs are small and there may only be a handful of them. ISPs must therefore establish an international private leased line to exchange traffic with a foreign Tier 1 internet backbone provider (IBP) in order to gain connectivity to the internet backbone, so that users would be able to access a website hosted on another network on the other side of the world. These Tier 1 IBPs are usually based in the USA or Europe. Like local leased lines, this international private leased line circuit (IPLC) can be provided by the national telephone company or another data communications operator, or can be gained independently by the ISP establishing its own satellite connection where they are licensed to do so. A local 64 Kbps leased line in the USA cost US$80 per month and twice that (US$190) in Kenya, whilst an IPLC from Kenya was charged at US$1,687 (some 21 times as expensive).

3 OECD, *Broadband Access for Business*, 2002 http://www.oecd.org

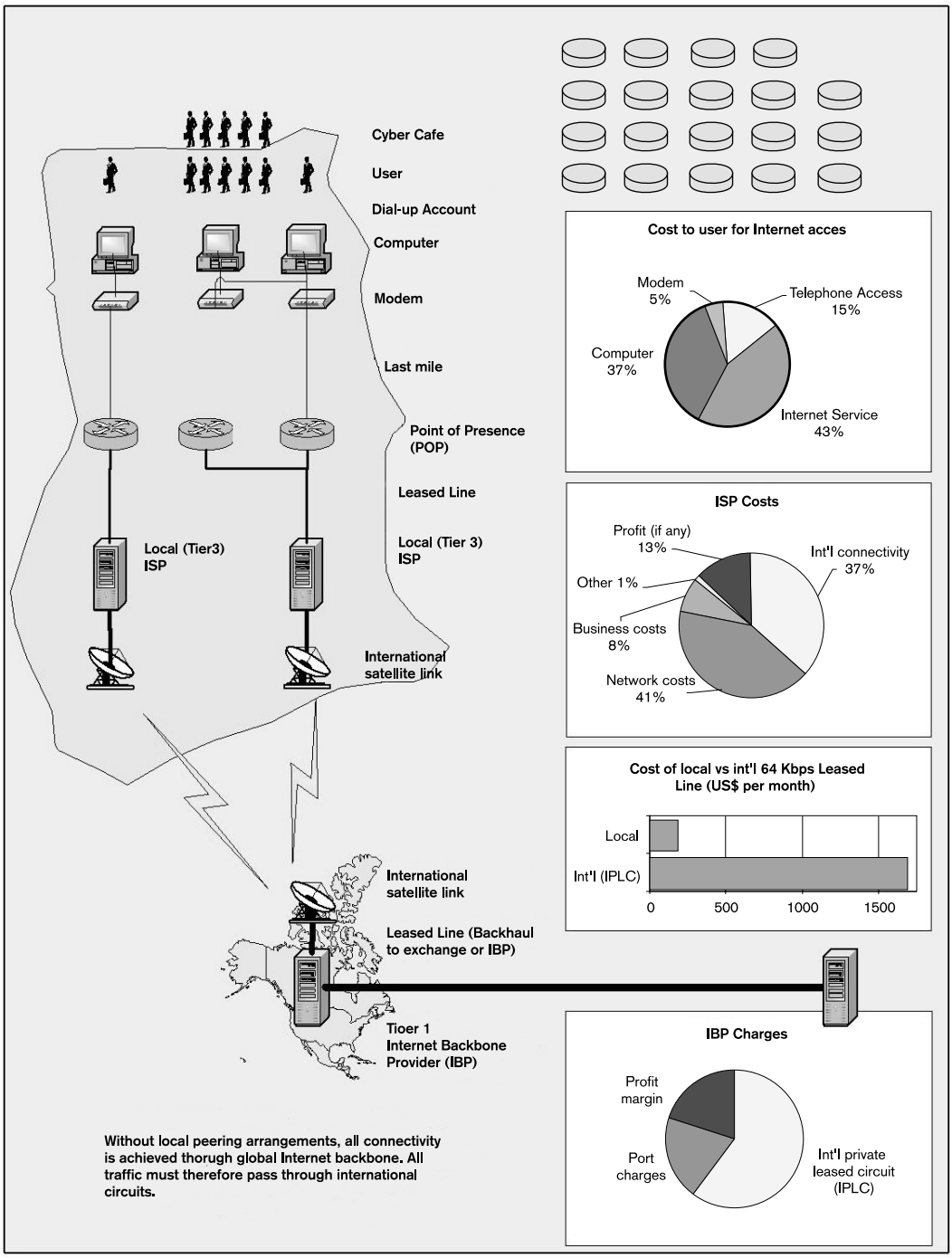
4 *ibid*

Cost of internet access in developed countries (eg Germany)



Sources: Broadband Access for Business, OECD (2002); Towards a Knowledge Based Economy, UNECE (2002).

Cost of internet access in developing countries (eg Ghana)



4. Market structure, monopolies and multinationals

Initially, internet service providers were non-profit organisations such as universities and research institutions. When the internet became a business in 1994, the number of ISPs increased enormously, but as time passed a process of consolidation took place, with many smaller ISP going out of business or being bought up by the larger ones. In broad terms, most ISPs started out selling 'retail'; in other words directly to customers. As the process of consolidation reshaped the industry, the larger internet connectivity providers began to 'wholesale' bandwidth to 'retail' ISPs; selling to those who service customers directly.

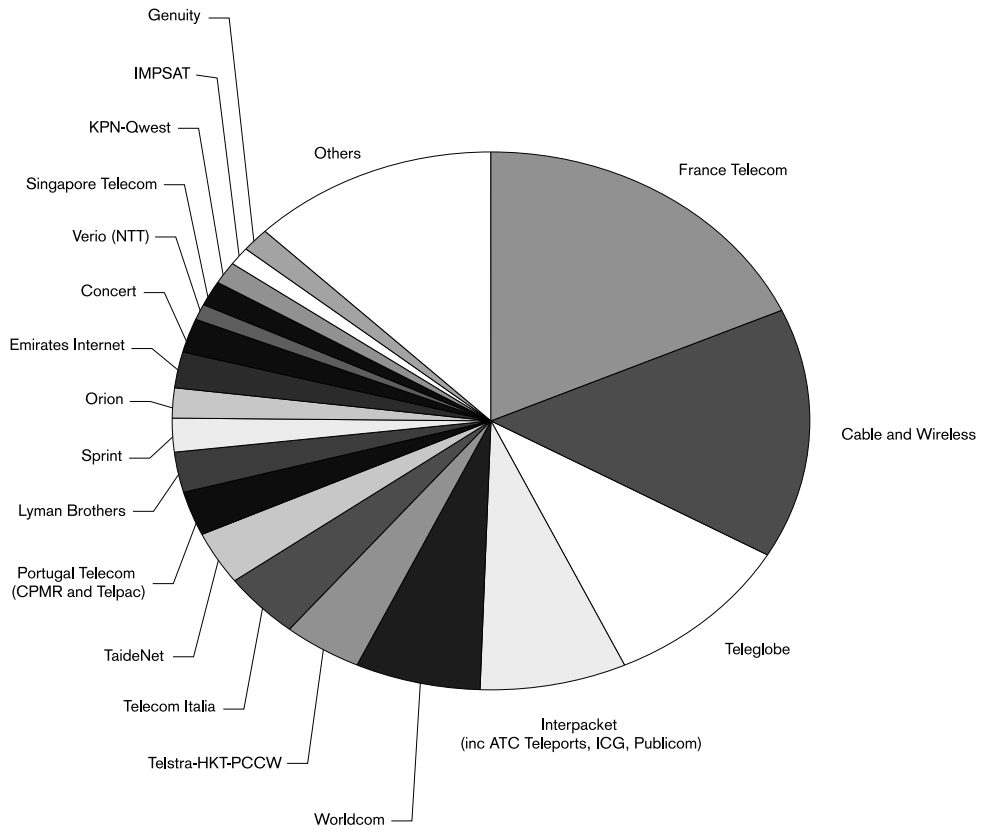
In order for any ISP to operate it has to buy upstream bandwidth connections to allow its customers to access web sites hosted in other countries or to send email between different countries. This has led to the development of a three-tier market structure, that mirrors the telecommunications industry.

Tier 1

The big fish at the top of the food chain

At the top level you have tier one, the internet backbone providers. These are the dozen or so international companies that own or lease the international infrastructure that links different continents, particularly the USA and Europe. The companies in this category include: AT&T, BT Ignite, Cable and Wireless, France Telecom and WorldCom.

With a few exceptions – such as the new and now troubled 'upstarts' (WorldCom) – these companies are the international telecom players who carry both voice and data traffic. And whilst there is intense competition for routes with heavy traffic (like those across the North Atlantic), there is less competition between carriers in a continent like Africa with a small flow of traffic, which



Source: OECD, Netcraft, Brian Longwe.

may increase the cost of bandwidth. The issue of who pays what for international traffic is important as outlined below:

Who should pay what?

Argument one: Bandwidth costs in Africa in the 1990s were characterised by telecommunications companies and internet operators extracting maximum return out of their positions in monopoly or partially liberalised markets. In today's liberalised markets in Africa, end user prices are broadly similar. In all cases service providers will cite their upstream bandwidth costs as their single biggest cost of doing business, and in all cases the average end user prices would be higher than prices in developed countries (particularly the USA and Europe).

When an end user in Kenya sends email to a correspondent in the USA it is the Kenyan ISP that bears the cost of the international connectivity from Kenya to the USA. When an American end user sends email to Kenya, it is still the Kenyan ISP that bears the cost of the international connectivity, and ultimately the Kenyan end user who bears the brunt by paying higher subscription fees.

The existence of reverse subsidies is the single largest factor contributing to high bandwidth costs. These reverse subsidies are costing the continent anything between US$250 and US$500 million per annum.

Argument two: The Internet Backbone Providers in the developed world respond that they do not charge developing country ISPs any more than their other customers. They believe that the majority of international costs are incurred for a number of reasons including: poor telecommunications infrastructure at a regional and national level, fewer peering points than elsewhere and a lack of genuine competition in most developing countries.

There is some evidence to support the contention about lack of competition. Ghana Telecom is part of a consortium that invested in a fibre cable and the members have a five-year monopoly, during which time they will recoup their investment before opening up the cable to other users. An E1 line (2.048 mbps) from Ghana Telecom using the new SAT3 fibre cable costs US$15,000 a month, approximately 60% of what it costs to buy equivalent satellite bandwidth. Nonetheless Ghana Telecom is responsible for the Accra-Lisbon section and that piece costs US$12,000 of the total price, the balance being international costs.

In any structure where there are relatively few providers, there are inevitably monopoly-related issues. The Tier 1 companies are at the top end of the 'food chain' and their pricing policies are bound to set the framework for what others can charge. There are both regulation and competition mechanisms at a national level in Europe, North America, Australia and New Zealand. There are a number of issues that remain to be tackled (such as the local loop) and the impact of regulation and competition policies obviously differs from country to country. However, the regulatory and competition agencies are arguably reasonably effective in dealing with the issues on which they choose to focus.

At a regional level, the European Union operates a competition policy that is often capable of tackling monopoly issues and ensuring fair play across member countries. For example, EU policy calls for members to unbundle the local loop. Whilst members are moving towards this goal at different speeds, it sets an effective overall competition objective. Outside these areas, it is much harder for a developing country to address international regulatory or competition issues, as there is no structure that has this function. In a continent like Africa, there is no way of mediating a dispute over rates or competition issues between say the powerful telecom company Telkom in South Africa and a small ISP in Lesotho. In several Eastern European countries, the old state company is now the de facto (private) monopoly.

In the days when nearly all telecommunications companies were government-owned, this role was the responsibility of the ITU which put in place the accounting rate system. With the involvement of governments, state-owned and private sector companies, its process of decision-making has been ponderous and its ability to address emerging international regulatory and competition issues almost non-existent. In addition, with the majority of voice and data traffic going through privately-owned companies, its influence over rates has waned to the point where accounting rates are no longer the benchmark for the sale of access to infrastructure that they once were.

Tier 2

National and regional providers

In the second tier, there are 50-60 providers who provide infrastructure at a national or regional level. Some, like COLT, chose to provide fibre links between cities in Europe with concentrations of financial services companies. Others, like Telewest and NTL, are cable providers. They have added internet access (along with telephony) in various forms to a service that was originally driven by offering 'pay-for' cable television channels.

A range of policy issues emerges at this level. For example in the UK the roll-out of ADSL is left largely in the hands of BT. The carrier dragged its heels over obligations to unbundle the local loop (ULL) and allow alternative operators access to its exchanges, and instead cut the wholesale price of ADSL to a range of different ISPs from £25 to £14.75 per month. As a customer you can buy an ADSL connection from a national ISP like Demon or Easynet, which charge less than £30 per month for broadband internet access. However if there are service issues, the ISP provider will often need to turn to BT as the underlying service provider to sort them out. Since BT controls the infrastructure and knows the number of customers each of its wholesalers has, it retains an unfair advantage in this new market. A similar process has occurred in some other European countries, such as Spain.

The same sort of arguments applies when an incumbent telecommunications company launches an ISP in a developing country. It has access to the details of the international bandwidth its competitors are buying from it. Using this it can work out each company's customer base and revenues. An ISP started in these circumstances is usually subsidised in a variety of ways by its parent company. It will be hard to establish the level of this subsidy unless the company has transparent accounting procedures and the ISP operation is separated out from the main company's other operations. Unless these issues are addressed by the regulator, there will not be a 'level playing field'.

At the international level, there is also the issue of whether there is a single monopoly provider for international bandwidth. In the UK, for example, a number of international providers operate, but in Kenya there is only one company that can be used – Jambonet, a subsidiary of the incumbent Telkom Kenya – the international access point for all ISPs in the country. A monopoly provider will usually keep prices high. Luckily for Kenyan ISPs, the new government has decided to open up this market to competition and will shortly license more international bandwidth providers.

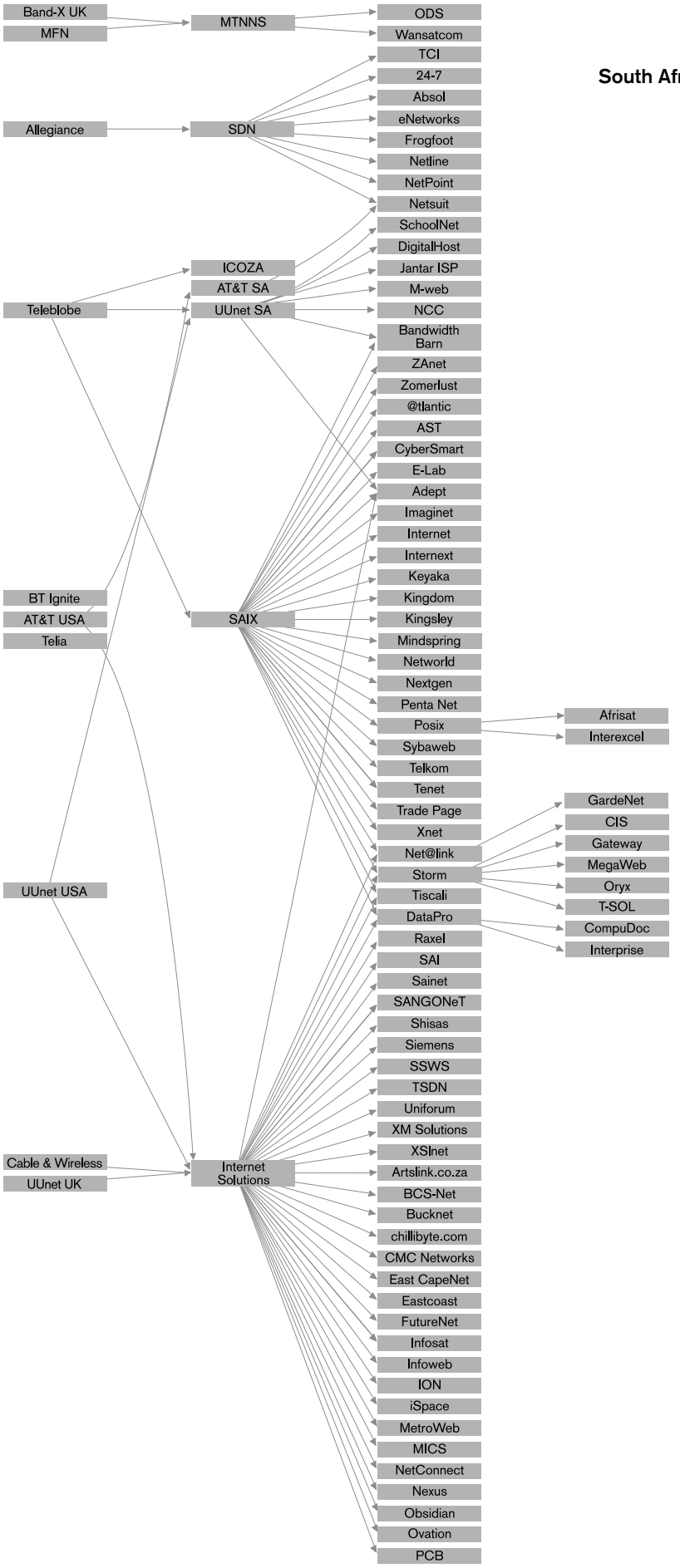
Tier 3

A multitude of ISPs

The third tier in the industry consists of ISPs that service customers directly, of which there are many thousands. However the number of companies that can be supported by the market in each country will vary enormously. Because the cost of bandwidth falls the more you buy, there is inevitably a tendency to consolidation. Initially there tends to be a large number of market entrants, each looking to establish themselves in what is seen as a new market opportunity. Over time the market consolidates with a much smaller number of players coming to dominate it.

In larger markets, a similar three tier structure is often in place. For example in South Africa there are over a hundred Tier 3 ISPs connected to five Tier 2 ISPs (MTNNS, SDN, UUNet SA, SAIX, and the Internet Solution), which in turn are connected to several global Tier 1 providers (Teleglobe, UUNet, Cable and Wireless).

South Africa's Hierarchy of ISPs



Source: Gregory Massel
http://www.ispmap.org.za

5. Networks interconnections and exchanges

The manner in which network interconnections occur lies at the heart of the economics of the internet. At each point where one network connects to another, there is a device called a router. Routers act like traffic signs, pointing the way to the IP address of the destination computer, and selecting the optimal route through the network using continually updated 'routing tables'. In this way, if one route is blocked, then packets will be redirected along another. There are different classes of router for different levels in the network hierarchy described above.

The technical level exists alongside a level of financial interaction between providers, which has important policy implications. Under the settlement system of the telecom world, cash flows from the core to periphery of the network; but, says Tim Kelly, head of the ITU's policy and strategy unit, in the internet world cash flows from the periphery to the core of the network[1] . Essentially, at each point of interconnection between two networks there is either a peering relationship (which is free) or a customer/supplier relationship (which is paid for).

Peering and transit: two different ways to interconnect

There are a number of different peering and transit arrangements that allow interconnection:

Private bilateral peering: Two ISPs negotiate a bilateral 'private' interconnection, using one or two leased lines, to exchange traffic between their networks. The term used for this is 'peering' because the interconnection takes place at the same level in the network hierarchy – the ISPs are peers. These exchanges are usually but not always free: the ISPs do not charge each other for traffic, and will split the costs incurred. In order to ensure there is no imbalance in the traffic flows, ISPs that enter peering relations are usually of similar size. Local (Tier 3) ISPs of equivalent size will therefore peer with each other, national or regional ISPs of equivalent sizes will peer with each other, and IBPs will peer with each other. The size of an ISP can be measured by the number of customers it has, the volume of traffic, backbone capacity, size and geographical reach of its network, or the number of content web sites.

In Europe, with so many different ISPs of different types, technical peering often involves a commercial transaction. The charges between two ISPs will depend on the relative size of each, which is measured according to a range of the factors mentioned above. Geoff Huston of Telstra describes how the peering discussions can develop[2] : "In many ways, the outcome of these discussions can be likened to two animals meeting in the jungle at night. Each animal sees only the eyes of the other, and from this limited input, the two animals must determine which animal should attempt to eat the other!"

A settlement-free peering relationship does not allow one ISP to transit traffic through a second ISPs network to an IBP, notes Clare Milne; this would be the equivalent of the first ISP piggy-backing on the network and paid-for transit agreed by the second ISP to the IBP.

Multilateral peering: In order to exchange traffic with as many networks as possible, it is beneficial therefore for as many ISPs as possible to share the same facility. These allow simultaneous peering between two or more Tier 3 ISPs. There are two types:

Internet Exchange Point (IXP): In order to achieve the most efficient interconnection, ISPs would seek to establish a point of presence (POP) or even locate their servers next to each other. Indeed, so-called collocation facilities provide exactly this under the same roof.

Internet exchange points (IXPs) are places where ISPs exchange traffic with one another. IXPs have rules guiding the interconnections, some are run on a not-for-profit basis as a consortium of local ISPs, and others are run on a commercial basis, where ISPs must pay to peer. As ISPs maintain POPs at such a facility, in commercially run IXPs customers pay the cost of a third party to manage the collocation facility (temperatures, uninterruptible power supplies, maintenance), typically by rack space (determined by how many racks they need to house their equipment).

There are over 150 IXPs around the world, examples of which are SAIX (South African Internet Exchange), the London Internet Exchange (LINX), Mae West, etc.[3]

Even when IXPs exist, they may not be a local company. In Brazil, for instance, there is one large IXP in São Paulo,

1 T Kelly, "Global Internet Connectivity and the Digital Divide", OECD Workshop on Internet Traffic Exchange, Berlin, 2001.

2 G Huston, "Interconnection, Peering and Settlements", Telstra Australia, at http://www.potaroo.net/papers.html or http://www.uixp.co.ug/interconnect.html

3 Telegeography list of IXPs: http://www.telegeography.com/resources/directories/internet/ix_directory.html; European IXPs: http://www.ep.net/naps_eu.html

run by an agency of the State of São Paulo government, which has 'given' it to a for-profit Miami-based operator. So the entire backbone traffic in Brazil is in the hands of a US company. This has implications for national sovereignty and control of national traffic.

Network Access Points (NAPs): A NAP has two distinct roles. It acts first as an exchange provider between Tier 3 ISPs that seek to enter into bilateral peering arrangements (an IXP), and second as a facility where Tier 3 ISPs purchase agreements with one (or more) Tier 1 internet backbone providers, which are also connected to the NAP. In this sense, Tier 3 ISPs gain access to the networks of larger IBPs.

Transit arrangement: In a transit arrangement, one ISP pays the other on a customer/supplier basis to carry its traffic. "Where a wholesale or retail service agreement is in place, one ISP is in effect a customer of the other ISP," says Geoff Huston of Telstra. "In this relationship, the customer ISP (downstream ISP) is purchasing transit and connectivity services from the supplier ISP (upstream ISP)."

Because they are businesses, IBPs peer with other IBPs for free, but will charge Tier 3 and Tier 2 ISPs for access to their network. "Negotiations for peering do not just occur horizontally between ISPs but also vertically between 'small local ISPs' and 'large national IBPs,' notes Clare Milne in the DFID Internet Costs Study report[4]. "In the latter case, the large national IBPs have a stronger bargaining position because they not only provide access to their customer and content base, but also act as a gateway to the rest of the Internet."

In a transit agreement, two charges are made. First, the downstream ISP pays a network access charges (called 'port charges'). Second, it pays for the capacity of the link (in Mbps) required. Under this customer/supplier relationship, connecting ISPs pay the full costs of the circuit to connect to the IBP. When international links are required, the downstream ISP therefore has to pay both halves of the international circuit, plus the costs to exchange the traffic. This happens even though the traffic then flows in both directions.

The issue of international internet connections has become highly controversial, as smaller ISPs in developing countries bear all the international costs of internet access. Transit arrangements inherently do not recognise the value that Tier 3 ISPs bring to the IBPs network (in terms of reciprocal access to their networks), despite the fact that onward connectivity is part of its onward proposition. Indeed, because ISPs pay all the cost to connect to IBPs (even though traffic flows in both directions), and an IBP in the USA will have multiple relationships with ISPs in different continents, it simply acts as a middleman offering connectivity to both third party networks and charging both in order to do so.

Yoshio Utsumi, Secretary-General of the ITU, summarised the situation during 2000: "At the moment, developing countries wishing to connect to the global internet backbone must pay for the full costs of the international leased line to the country providing the hub. More than 90% of international IP connectivity passes through North America. Once a leased line is established, traffic passes in both directions, benefiting the customers in the hub country as well as the developing country, though the costs are primarily borne by the latter. These higher costs are passed on to customers [in developing countries]. On the internet, the net cash flow is from the developing South to the developed North."

In 2000, ISPs in Asia Pacific argued that they were paying a total of US$5 billions per year to IBPs in the US, and in 2002 African ISPs were paying up to US$500 millions a year. "The existence of reverse subsidies is the single largest factor contributing to high bandwidth costs," says Richard Bell in his paper *Halfway Proposition*[5], "these reverse subsidies are costing the continent anything between US$250m and US$500m per annum".

On the one hand, ISPs and internet users outside North America argue that they are effectively subsidising US ISPs and their customers. European ISPs first brought the issue up in the mid 1990s, followed by Asian ISPs[6], and now developing world ISPs are doing the same. On the other hand, IBPs in developed countries argue that they do not discriminate against developing countries. Rather, the bulk of the costs are incurred over the international leg because of geographic remoteness, the lack of telecommunications infrastructure and the lower levels of competition in developing countries. In both Europe and Asia, the circumstances have been mitigated considerably as ISPs have created national and regional IXPs, which reduce the importance of the middleman providers.

Convergence – internet telephony, radio, literature, music, etc

Another key issue is that of technological convergence, whereby different types of traffic are carried on the same

4 C Milne, Antelope Consulting, http://www.clairemilne.btinternet.co.uk/telecommunications_development/DFID_internet_cost_report.htm

5 R Bell, "The 'Halfway Proposition'", African ISP Association, at http://www.afrispa.org/Initiatives.htm

6 "International Charging Arrangements for Internet Services (ICAIS)" at http://www.apectelwg.org

internet protocol (IP) platform. Not only can different types of content be digitised, and then sent as packets (such as scanning photos and emailing them), but increasingly content is produced in digital form. Such content includes radio, literature, music, film, or games. Users can download these products over their internet connection rather than purchase them through retail outlets. The internet is an excellent distribution system: because it appears free to the user, and the links are paid for through bilateral or multilateral settlements between ISPs, the cost of distance has collapsed. In this way online radio stations, for example, can broadcast globally without the expense of transmitters, and online newspapers can charge readers subscriptions without having to print and deliver the newspaper. For the internet distributor, the only major expenses are the bandwidth of the leased line and server capacities that are required to cope with the volume of requests for data from that website.

The classic example is voice traffic. Internet telephony exploits the fact that, when carried over the internet, voice traffic bypasses the accounting rate system built up around the circuit-switched network. It works on the principle that network connections are free, and uses the public internet as its means of transmission. A user can send an email without directly having to pay any costs to transport it across the world, and the same applies for packets that carry voice conversations. In the digital circuit-switched network, each call sets up a dedicated channel through the network for the duration of the call (including all the silences) and consumes a bandwidth of 64 Kbps. In a packet-switched network, each call consumes around 16 Kbps and when there is no activity (during silences), no packets are sent.

Internet telephony has developed through a number of different stages, from PC-to-PC telephony, to PC-to-phone telephony, to phone-to-phone telephony. It is particularly attractive to customers because the tariffs for international voice calls can be very expensive. However, the quality of calls has been a key issue because, unlike data streams which when delivered by the internet arrive by different routes in a different order and are then reassembled, in order to be intelligible voice conversations require a constant stream. Otherwise there is an echo, words get scrambled and some words do not arrive at all. Internet telephony is technically distinct from Voice over Internet Protocol (VoIP), which uses a private managed IP network in order to control the quality of the transmissions. Because of the efficiency of sending voice over an IP network, an increasing number of telephone companies are now using VoIP to carry their international traffic. By doing so they can squeeze much more traffic into the same international link.

Another example is the distribution of illicit or grey market products over the internet. Because of the lack of centralised governance over the internet, it is not only easier to evade detection but also harder to define jurisdictions and therefore to prosecute. The pornography industry, for example, has long exploited the global distribution powers of the internet, and the manner of delivery – such as (relative) anonymity. Indeed, the pornography industry has been at the forefront of the development of some technologies such as video conferencing and online electronic transactions. Another example of this is Napster, which allowed users to download MP3 music files for free and in so doing bypass commercial distribution outlets. Applications such as these use peer-to-peer (P2P) software, essentially a networking programme which allows a group of users to connect to each other's computers and access files from each other's hard drives. These work by allowing users to share files through swapping corresponding IP addresses of each other's computers. The post-Napster p2p systems are extremely decentralised, with users' own computers acting as the databases, and they work separately from, though often in collaboration with, the Web.

6. Regional differences: Africa, Asia, Europe, USA

Comparisons of internet costs between Asia, Europe and the USA, allow us to identify the key differences between regions in terms of internet costs:

- The cost of internet access is much lower in developed countries than in developing countries. For example, the total cost of internet access in Singapore (US$10.56 per month) is much lower than the cost in Kiribati (US$143.73). this is due to lower prices for leased lines, less need for international transit, local peering, etc. in developed countries.
- In Singapore, internet access is equivalent to 0.5% of monthly GDP per capita. By contrast, in Kiribati, a group of 33 coral atolls in the Pacific Ocean, internet access costs 3.38 times the average monthly income. In relative terms therefore, it is much more expensive for someone living in a developing country to access the internet than in a developed country. If people were prepared to spend as much as, say, 5% of their monthly income on internet access, then it would be affordable only in 11 out of 35 countries in the Asia Pacific region).
- Because of the need for direct international internet connections between Tier 3 ISPs in developing countries and internet backbone providers, wealth flows from the developed periphery to the developed core.
- The affordability of internet access is directly correlated with the level of internet penetration[1]. The table below shows that the countries with the lowest cost internet access generally have the highest penetration. In Australia, where 37% of people are internet users, the cost of internet access is 1.1% of monthly income. In Papua New Guinea where 0.98% of the population are internet users, internet access costs 8 times the average monthly income.
- Obviously where there are disparities of wealth within countries, the less well-off are less likely to use the internet. The digital divide then finds expression along other economic (rural/urban) and social (age, gender) axes.
- In addition to wealth, the digital divide is caused by three factors: local call rates and leased lines rates are kept (artificially) high in unliberalised markets; the structure of the internet which forces ISPs in developing countries to connect to the internet backbone through international links, and; the cost of international bandwidth.

1 M Rao has devised a scheme for classifying countries from the viewpoint of the Information Society at http://www.itu.int/osg/spu/visions/developing/paper1.html

Table 1. Asia Pacific: Comparison of internet costs, income and internet penetration ranked by cost of monthly internet access

Country	ISP subscription (per month in US$)	Telephone call charge (per month in US$)	Total cost of internet access	GDP per capita (US$)	GDP per capita per month (US$)	Cost of internet access as % of GDP per capita	Internet penetration (%)
Singapore	0	10.56	**10.56**	23137	1928.1	**0.5**	**36.3**
New Zealand	11.74	0	**11.74**	13311	1109.3	**1.1**	**28.57**
Malaysia	5.26	7.11	**12.37**	3869	322.4	**3.8**	**27.31**
Macau	13.54	0	**13.54**	14078	1173.2	**1.2**	**22.54**
China	9.78	4.35	**14.13**	834	69.5	**20.3**	**2.56**
India	5.98	10.17	**16.15**	459	38.3	**42.2**	**0.68**
Australia	15	3.42	**18.42**	19987	1665.6	**1.1**	**37.13**
Tonga	18.87	0	**18.87**	1504	125.3	**15.1**	**2.83**
Nepal	13.34	6	**19.34**	239	19.9	**97.1**	**0.26**
Philippines	19.42	0	**19.42**	977	81.4	**23.9**	**2.55**
Pakistan	9.69	10.17	**19.86**	427	35.6	**55.8**	**0.35**
Sri Lanka	5.59	14.77	**20.36**	882	73.5	**27.7**	**0.8**
Brunei Darussalam	22.19	0	**22.19**	13175	1097.9	**2.0**	**1.04**
Hong Kong SAR	17.69	4.62	**22.31**	24136	2011.3	**1.1**	**38.48**
Indonesia	11.45	11.4	**22.85**	738	61.5	**37.2**	**1.91**
Vietnam	15.89	7.21	**23.1**	393	32.8	**70.5**	**1.24**
Korea	23.24	0	**23.24**	10036	836.3	**2.8**	**52.1**
Thailand	5.4	20.3	**25.7**	2018	168.2	**15.3**	**5.77**
Bangladesh	12.9	18.28	**31.18**	351	29.3	**106.6**	**0.19**
Guam	35	0	**35**	22086	1840.5	**1.9**	**30.53**
Fiji	38.75	1.58	**40.33**	1788	149.0	**27.1**	**1.82**
Lao PDR	33	9.05	**42.05**	325	27.1	**155.3**	**0.18**
Japan	42.07	0	**42.07**	37544	3128.7	**1.3**	**43.93**
Bhutan	30.73	12.71	**43.44**	715	59.6	**72.9**	**0.43**
Taiwan	47.08	0	**47.08**	13819	1151.6	**4.1**	**34.9**
Samoa	29.09	20.69	**49.78**	1330	110.8	**44.9**	**1.67**
Papua New Guinea	25.96	26.55	**52.51**	78	6.5	**807.8**	**0.94**
Iran	40.39	12.93	**53.32**	5181	431.8	**12.3**	**1.55**
Maldives	65.36	0	**65.36**	1978	164.8	**39.7**	**3.64**
Vanuatu	75.7	0	**75.7**	1148	95.7	**79.1**	**2.73**
French Polynesia	24.75	57.37	**82.12**	16834	1402.8	**5.9**	**6.76**
New Caledonia	29.89	53.8	**83.69**	14250	1187.5	**7.0**	**11.35**
Cambodia	67.4	18	**85.4**	257	21.4	**398.8**	**0.07**
Solomon Islands	119.34	0	**119.34**	579	48.3	**247.3**	**0.46**
Kiribati	140.93	2.8	**143.73**	509	42.4	**338.9**	**2.32**

Source: ITU, "Asia Pacific Telecommunication Indicators", 2002.

Wealth is probably the most important feature of regional differences. In a league table, the Americas and Europe would appear at the top, followed by Asia, with Africa at the bottom of the league. Obviously there are wide disparities of wealth within regions, and these can be identified by looking at 60 selected countries in Table 2 below. However, there are a number of other factors that affect internet take-up.
These include:

- The degree to which markets are liberalised. For example, Ethiopia's low level of internet users can in part be explained by the fact that its telecom and internet delivery is entirely state-controlled.
- The slow rate of roll-out in particular countries faced with particular geographical challenges: for example the GDP per capita in Haiti and Nigeria is similar but the rate of internet penetration in the former is 0.36% as against 0.09% in Nigeria. Haiti is a relatively small island whereas Nigeria is a big country.
- Even in countries with policies designed to promote internet use, the outcomes can be very different. In South Korea there is 52.1% internet penetration (comparable to US and European levels) whereas in Singapore it is only 36.3%, even though the latter has a higher GDP per capita. The difference may partly be explained by differences in political culture.

Table 2. Wealth and internet users 2001 (60 selected countries), sorted by region and ranked by internet penetration

Country	GDP per capita (US$)	Internet users ('000)	Internet penetration (%)	Country	GDP per capita (US$)	Internet users ('000)	Internet penetration (%)
Asia	**2,298**	**156,897.8**	**4.34**	Ghana	209	40.5	**0.19**
Korea	10,036	24,380.0	**52.1**	Burkina Faso	200	19.0	**0.16**
Japan	37,544	55,930.0	**43.93**	Sierra Leone	152	7.0	**0.14**
Hong Kong SAR	24,136	2,601.3	**38.48**	Nigeria	434	115.0	**0.09**
Australia	19,987	7,200.0	**37.13**	Mozambique	202	15.0	**0.07**
Singapore	23,137	1,500.0	**36.3**	Ethiopia	106	25.0	**0.03**
Taiwan	13,819	7,820.0	**34.9**	**Americas**	**15,323**	**182,942.3**	**21.81**
New Zealand	13,311	1,091.9	**28.57**	United States	35,843	142,823.0	**50.14**
Thailand	2,018	3,536.0	**5.77**	Canada	23,484	13,500.0	**44.98**
China	834	33,700.0	**2.56**	Chile	4,314	3,102.2	**20.14**
Philippines	977	2,000.0	**2.55**	Peru	2,071	3,000.0	**11.49**
Kiribati	509	2.0	**2.32**	Argentina	7,418	3,300.0	**9.11**
Indonesia	738	4,000.0	**1.91**	Venezuela	5,017	1,264.7	**5.13**
Fiji	1,788	15.0	**1.82**	Brazil	2,922	8,000.0	**4.65**
Samoa	1,330	3.0	**1.67**	Bolivia	963	150.0	**1.81**
Iran	5,181	1,005.0	**1.55**	Guatemala	1,757	200.0	**1.71**
Vietnam	393	1,009.5	**1.24**	Cuba	1,518	120.0	**1.06**
Papua New Guinea	78	50.0	**0.94**	Haiti	423	30.0	**0.36**
Sri Lanka	882	150.0	**0.8**	**Europe**	**11,428**	**147,269.2**	**18.4**
India	459	7,000.0	**0.68**	Iceland	26,617	195.0	**67.94**
Solomon Islands	579	2.0	**0.46**	Norway	37,116	2,700.0	**59.62**
Pakistan	427	500.0	**0.35**	Denmark	30,146	2,900.0	**54.03**
Africa	**723**	**6,781.2**	**0.85**	Sweden	23,546	4,600.0	**51.62**
Mauritius	3,771	158.0	**13.25**	UK	23,694	24,000.0	**39.95**
South Africa	2,542	3,068.0	**7**	Germany	22,267	30,800.0	**37.36**
Kenya	338	500.0	**1.59**	France	21,737	15,653.0	**26.37**
Egypt	1,528	600.0	**0.93**	Poland	4,572	3,800.0	**9.83**
Tanzania	271	300.0	**0.83**	Bulgaria	1,672	605.0	**7.46**
Cote d'Ivoire	563	70.0	**0.43**	Latvia	3,213	170.0	**7.23**
Cameroon	615	45.0	**0.29**	Belarus	1,223	422.2	**4.11**
Mali	236	30.0	**0.26**	Russia	1,709	4,300.0	**2.93**
Zambia	312	25.0	**0.23**				

Source: ITU.

7. Technical infrastructure of the internet and how it shapes governance

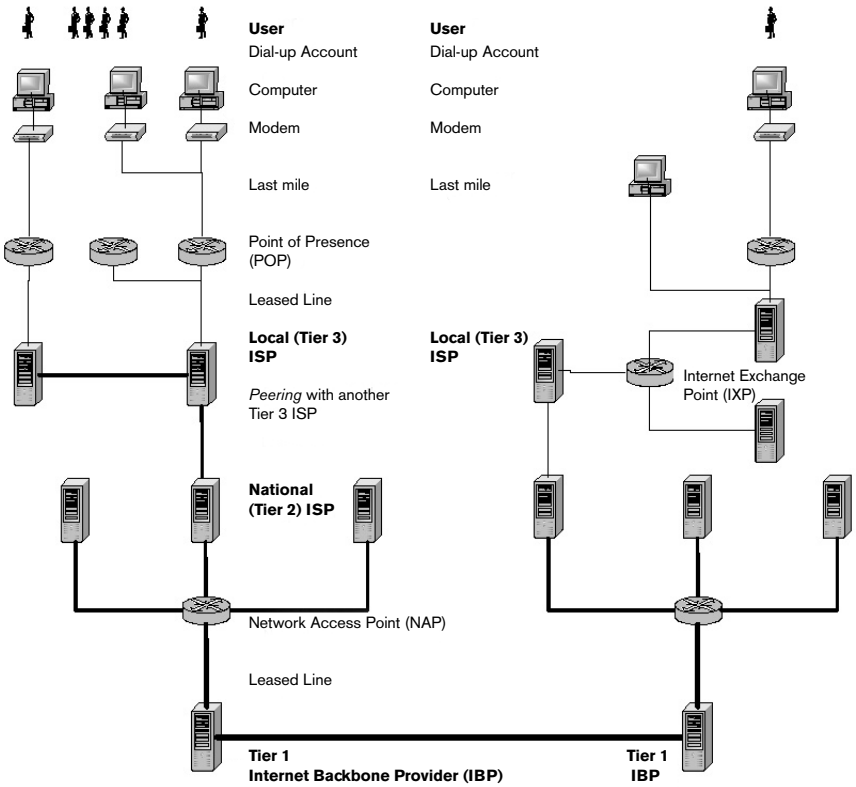
Internet underpinned by telecommunications

The telecommunications network, based on circuit-switching, has highly regulated structures. At the national level, each country has a ministry, laws surrounding the use of networks, and in a growing number of cases an industry regulator. There are also overarching international bodies like the International Telecommunications Union (ITU, a specialised agency of the United Nations) and the European Union, which regulate the sector in different ways. Policy is made at these different levels, and stakeholders can make an input into it.

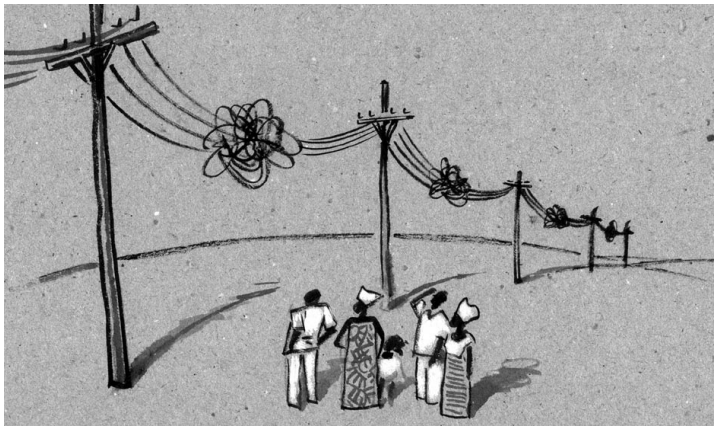
For example, the cost of international telephone calls is met through a regime of bilateral settlements called the international accounting rate system. This is the mechanism for sharing the cost for international calls between the sending and receiving carriers in each country, so that each side pays half of the cost of the international circuit. Because these accounting rates vary from the actual cost of that circuit (this cost has fallen), and given the historic imbalance in traffic between developed and developing countries, this accounting rate mechanism tends to redistribute revenue from the core of the world economy (developed countries) to the periphery (developing countries). As a result, the accounting rate system is no longer the centrally set benchmark for rates that it once was. Where liberalisation has occurred, the market decides.

As it is not feasible for one ISP to maintain bilateral interconnections with every other ISP, and with the growth of the internet, the hierarchical structure described above has emerged between service providers. In this structure, the local ISP (Tier 3) will exchange traffic with a regional or national ISP (Tier 2), which in turn will exchange traffic with a global internet backbone provider (IBP) (Tier 1). A Tier 1 IBP is defined as having its own international backbone infrastructure, which is high capacity fibre-optic or satellite links. With internet traffic often travelling around the world it will typically be routed from a Tier 3 ISP up to a Tier 1 IBP for the main global transport, and then routed back through the other side of the hierarchy to its destination.

Basic technical infrastructure of the internet



The local ISP operates a leased line from the POP to its central node, and then on to another ISP in order to exchange traffic with each other. That ISP in turn exchanges traffic with other ISPs, which in turn have relationships with additional ISPs. In this way, data from one machine can reach another on the other side of the world, and every machine connected to the internet is theoretically connected to every other.



Internet governance

The internet is decentralised, self-regulating and has become increasingly driven by market forces. In contrast to the traditional telephone system, it is based on packet switching and has developed outside that system's highly regulated structures. As it is based on the technical and commercial interactions between a myriad of internet service providers (ISPs), internet economics is like an ecosystem in which the behaviour of each ISP is shaped by the market forces of these interactions. The opportunity for direct policy inputs is therefore much lower, and the most meaningful interventions are those with commercial relevance. However there remain fierce debates over its level of inclusiveness and its overall effectiveness.

The global nature of the internet, and its growth outside of the control of governments, have meant that there is no international internet governing body. The closest thing to international internet governance is therefore comprised of technical bodies, ranging from the engineering side, such as the Internet Engineering Task Force (IETF), to other technical areas such as responsibility for allocating domain names (the Internet Corporation for Assigned Names and Numbers – ICANN), and IP addresses (Internet Assigned Numbers Authority – IANA), or organisations which set generally recognised standards such as W3C. These and other organs of internet governance are discussed in Part 3.

A key example of internet governance in operation is the allocation of Internet Protocol (IP) addresses – akin to a telephone number for each phone, the unique address for every machine connected to the internet. When a user opens a dial-up internet account, the ISP gives it an IP address. Four Regional Internet Registries (RIRs) do this in each region: APNIC (the Asia Pacific Network Information Centre), ARIN (the American Registry for Internet Numbers), RIPE NCC (the Réseaux IP Européens Network Coordination Centre), and LACNIC (the Latin American and Caribbean Internet Addresses Registry). The Africa region is currently served by APNIC, ARIN and RIPE NCC, but a fifth RIR has been proposed for the region called AfriNIC. According to the Internet Society[1], these RIRs are "not-for-profit, member-based organisations that facilitate the development of consensus-based policies in a bottom-up, industry self-regulating manner in response to the requirements of the many and varied stakeholders in their respective communities. The RIR structure provides service in a fair, responsive, neutral, and impartial manner".

So the scope for policy interventions is lower with the internet, but because each of the millions of links of the internet are underpinned by the telecommunications infrastructure, decisions made in the telecommunications sector have profound effects over the internet. In particular the tariffs charged by telecommunication companies, and the licensing regime in a given country have direct impact on the costs of the internet and therefore the behaviour of ISPs. This in turn directly affects its cost relative to local incomes and how many people can have access, and is therefore a key area for policy inputs. Indeed, tariffs and the level of liberalisation are closely linked.

The most extreme example is countries where only one ISP has been licensed, and is run by the state. Often closed states, which do not wish their citizens to have access to information, seek to maintain their monopoly for political purposes, so that they can filter or control the flow of information that is available to citizens. In such countries, the 'internet' is essentially a single wide area network (WAN), which can be managed and controlled in the same way that a company or school network may wish to prohibit certain type of information (such as swear words or pornography).

Control of internet user behaviour is not limited to official governance structures. There are other aspects of control of the internet which are not strictly governance, but which do play an important part in regulating internet activity, such as laws on the protection of intellectual property, data and consumer protection, the distribution of pornography, etc. Often these do not refer specifically to the internet, but their application to the world of cyberspace is problematic because of the new ways in which data can be transferred. Some of these are discussed in Part 4 of this book.

---

1 ISOC, "The Regional Internet Registry Development Process", Member Briefing No. 10 December 2002, at http://www.isoc.org/briefings/010/index.html

8. Market models for extending access

This section looks at how different types of business practice and regulatory models can affect internet growth. It takes four examples that affect different aspects of infrastructure: free ISPs, internet exchange points, Voice Over IP (VOIP) and the use of cyber-cafes where individual computer purchase is too expensive.

Grameen Telecom's Village Phone Programme: A Multi-Media Case Study

GrameenPhone is a commercial operation providing cellular services in both urban and rural areas of Bangladesh, with approximately 40,000 customers. A pilot programme of GrameenPhone, through the Grameen Bank and a wholly owned subsidiary called Grameen Telecom, is enabling women members of the Grameen Bank's revolving credit system to retail cellular phone services in rural areas. This pilot project currently involves 950 village phones providing telephone access to more than 65,000 people. Village women access micro-credit to acquire digital GSM cellular phones and subsequently re-sell phone calls and phone services within their villages. Grameen Telecom staff have announced that when its programme is complete, 40,000 Village Phone operators will be employed for a combined net income of $24 million USD per annum.

In rural areas where isolation and poor infrastructure services are often the norm, telecommunications can play an extremely important role in enhancing rural social and economic development. Grameen Telecom's Village Phone programme provides an excellent opportunity to learn more about how private sector development (PSD) in the telecom sector can make a significant contribution to poverty reduction. The Village Phone programme also provides an opportunity to review innovative strategies for incorporating targeted, micro-level PSD in the telecom sector within project design. Documentation of the impacts of Grameen Telecom's Village Phone programme and its innovative approach to poverty reduction provide valuable learning and case study materials that can contribute to strategies for improved success in poverty reduction.

Source: http://www.telecommons.com/villagephone/contents.html

Free ISPs – sharing call revenues

The free ISP model originated in the UK, when the regulator OFTEL decided that the incumbent telecommunications company BT had to share revenues with ISPs. The basis for free ISPS is simple: the ISP and the company split the revenue from the call made to access the internet, at an agreed rate. It allows the ISP to offer its service for free or nearly free and the company gets a percentage of the large amount of extra traffic generated. In the UK free services attracted millions of users and therefore pulled in a considerable amount of new traffic. The largest of these – Freeserve – is now one of the largest ISPs in the UK with 2.6 million subscribers.

When Egypt's Ministry of Communications and Information Technology (MCIT) wanted to spread internet technology across the country, it announced a free internet access initiative based on the revenue-sharing model. In partnership with licensed ISPs, the government-owned Telecom Egypt has set up an estimated 15,000 ports, capable of serving 2 million internet users. Those taking up the service have to make a local phone call for access; no subscription is needed to access the net.

The user only dials his or her favourite ISP and gets access immediately. The cost of the call is shared between the ISP and the telecom operator, 70% and 30% respectively. The cost of one hour's connection is one Egyptian pound (about US$ 0.22). There is a wide range of different ISPs who cover 90% of Egypt's inhabited areas and the number of users is around 1 million, with most concentrated in the cities of Alexandria and Cairo.

Kenyan internet service provider Swift Global has launched a free ISP in conjunction with fixed-line operator Telkom (Kenya) and Interactive Media Services. Branded 'Internet Direct', the service allows users to access the internet without having to subscribe to an ISP. The revenue generated through this premium rate telephone number is shared between the three partners.

Another variant is the free ISP service from MTN in Uganda. Its fixed line customers can now dial up to the ISP of their choice and but do not need to pay monthly ISP charges or any initial connection fees. According to Erik van Veen its Chief Marketing Officer: "The basic premise of the product is that, in collaboration with ISPs, MTN has bundled the telecoms and ISP costs into a 'per minute' dial-up rate."

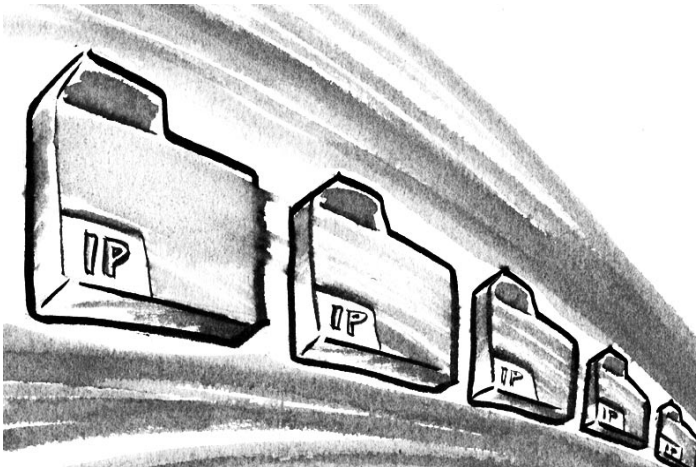
Sharing of revenues in this way is one of a number of regulatory approaches that can be used to encourage the growth of internet usage. Another approach is unmetered usage. In 2001 UK regulator Oftel insisted that the incumbent telecommunications company BT of-

fer unmetered access to the internet at a fixed price. It noted at the time that unmetered call durations are, on average, four times longer than metered call durations. Unmetered access requires available capacity but a fixed price, and it encourages greater usage.

In the developed world, users are accustomed to ringing a nationally available number at local call rates. However in many developing countries (particularly in Africa) numbers of this kind have not been introduced. In these circumstances, the unfortunate user has to pay long-distance rates to connect to the internet. A simple change in the regulatory framework can bring about its introduction.

IXPs, RXPs and international peering

The issue of the cost of international connections has already been raised. For example, in most African countries if you send email across town it makes a long and circuitous journey to North America or Europe before going back to its intended recipient. It costs money in international connectivity charges and gives latency problems (a fractional but sometimes problem-causing delay).



Local internet exchange points (IXPs) allow one country to route all (or most of) its internal internet traffic at a national level, thus saving money and adding speed to the connection. IXPs are the keystone of the entire internet economy: they interconnect different parts of the internet and they allow different ISPs to connect with each other, creating in effect a clearing house. Routing traffic the long way around is not an efficient way to use the network and thus the IXP mantra 'keep local traffic local' developed.

Local IXPs offer both internet users and ISPs a number of distinct advantages:

- They improve quality by speeding up connection times: there is a 200-900 millisecond delay in each hop the message makes across the system, compared to 5-20 milliseconds locally.
- They save money because the calling costs are all at a local level.
- They create new revenue opportunities because, for example, local content providers can start creating things like locally hosted web sites, a range of e-services and streaming. The latter would not be feasible if an international connection had to be made.

When Pacific Rim countries found in the 1990s they were paying far more than they were happy with for international connectivity, their approach was to say: Why do we need to get to the USA anyway? Most of our trade is national or regional. If we all peer our traffic within our countries and then within our regions we can dramatically reduce our connectivity costs.

Consequently, local and regional connectivity increased, international connectivity decreased and costs came down. In the process, the internet backbone providers found that the quality of connectivity that they were offering their customers in domestic markets was being reduced. The only way for them to maintain the quality was to establish Points-of-Presence (POPs) at the national and regional peering points in the Asia Pacific region. The internet backbone providers now bear the international connectivity costs, not the Asia Pacific ISPs (it is interesting to note that the Korean Internet Exchange Point is today the largest in the world). This shows how this approach can address international cost issues.

Africa is at a much earlier point in this cycle. The Kenyan IXP went online fully in 2002 with initially four ISPs but is now used by 10 of them. On an uncongested link, the latency is now 30-60 milliseconds. One rather conservative ISP decided that it would only require a 64k circuit to handle likely traffic and within two hours it was so packed that it got congested. Before it was established, international connectivity charges were nine times more expensive than local costs. Within a very short period of time Telkom Kenya had slashed its international call rates in half.

There are now six IXPs in Africa: South Africa, Zimbabwe, Nigeria (Ibadan with only two ISPs), Mozambique, Egypt, and the Democratic Republic of Congo (the last three opened recently). More are promising to open in the near future.

The major issue is one of trust. ISPs need to be able to work with their competitors and in some countries this level of trust has not yet been established. As Brian Longwe of the African ISP Association told a workshop at the Southern African Internet Forum: "Getting any IX/peering arrangement off the ground is 10% technical work and 90% socio-political engineering." He also pointed out the importance of getting ("written") regulatory support. Setting up a local IXP is neither costly nor difficult.

Once there is enough traffic, continental exchange points develop. The more you aggregate traffic, the better the deal you will get. For example, if Africa were to develop a continental peering point it would not have to pay to interconnect to the rest of the internet. It would be of a similar standing in the network hierarchy to a Tier 2 ISP or Tier 1 internet backbone provider and would therefore 'peer' with other equivalents.

VOIP – Challenging the incumbents

The convergence between voice and data is a development that is having a particularly significant effect upon the relationship between ISPs and incumbent telecommunications companies, particularly in Africa.

VOIP stands for Voice Over Internet Protocol and is sometimes used as a shorthand for internet telephony: in other words calls made over the internet. International VOIP minutes are estimated to have tripled in 2002. International Data Corporation (IDC), a market research firm, says that by 2004, VOIP minutes (retail and wholesale) and revenues will grow to approximately 135 billion minutes and approximately $20.7 billion, respectively, representing estimated compound annual growth rates of over 100%. Beyond cost savings, IP technologies will further the potential for the internet to become the preferred medium for both communications and commerce.

As a result, the internet is expected to carry a growing volume of US and international long distance voice traffic says IDC. Other analysts forecast that, by 2004, IP telephony will account for between 25% (Analysys) and 40% (Tarifica) of the global international voice traffic (compared to an estimated 3% of the total in 2000).

In Africa, VOIP is used 'illegally' by ISPs and cyber-cafes to offer international calls to people at much cheaper rates than charged by telephone companies. Because there is an enormous gap between the cost charged for international calls and what it actually costs to buy the connection, 'grey market' operators are exploiting the price difference.

As this takes calls away from national companies, most governments and regulators try to police the market. For example there are periodic police raids and the confiscation of equipment in Kenya and Ethiopia. In Ghana at one point the government even jailed some ISP owners for a short period of time. VOIP calls are difficult (but not impossible) to detect unless there is a large volume of calls. As a result the grey market often makes up 10-15% of the market in most African countries. In the case of Ghana Telecom, the company has estimated that it is losing some-

where between US$15-25 million a year in international call revenues to the grey market.

Why does this matter? Because the internet is creating new (often not currently legal) ways of doing business in developing countries. Regulators will need to consider whether they open up the monopoly on international call termination, and whether they involve those currently in the internet business. In the long-term there will be a shift from analogue to digital calling that will in large part use the internet. Developing country telecommunications companies need to plan for this transition now. It brings some advantages: for example, the cost of switching equipment is cheaper and it may help ease network congestion.

Cyber cafes: Access without owning a PC

As we will explore in chapter 9, the internet is a relatively expensive service to access for those with low incomes. In most developed world countries, large numbers of people have access to a laptop or PC, either at home or at work. But for those with low incomes or people on the move, cyber cafes that offered relatively cheap access were a natural extension of the industry. Places like Easyeverything offer internet access at US$1 per hour. Tourists and students formed a substantial part of the initial users attracted.

In countries where the cheapest PC (US$200-300) can be a substantial portion of the average annual earned income, the role of cyber cafes is particularly important. Without them, the number of people using the internet would be substantially smaller. Almost all African cities now have a wide range of internet cafes that offer access for between US$1 and US$5 an hour.

The cyber café allows users to control their own costs and enables them to walk in straight off the street without having to pay for their own machine. A similar approach to cell phones is the selling of pre-paid scratch cards for the internet. The user scratches to obtain a number, which he or she then dials. No dial-up account is necessary and the number allows the user a pre-allocated amount of time online.

In developing countries, the users of these cyber cafes tend to be young and are often former students who had access to the internet at university. They are mainly used for email: many users communicate with friends and relatives in the growing African diaspora worldwide. However there is increasing use of the internet, which may challenge existing values: young women in some African countries search for husbands in the developed world. Other uses are illegal: there is a growing level of internet card fraud where buyers use fake credit card numbers and get goods delivered to accomplices in the United States.

Cyber cafes are an excellent way of creating access in large population centres and are spreading to smaller towns, particularly in tourist areas. However in rural areas there are two particular problems. First, it is hard to get the density of people required to create a sustainable user base. Second, if it is a poor rural area, people there may not be able to afford using even quite low-cost facilities. These issues are explored in chapter 9.

The recurrent issue in policy terms is: who pays for the infrastructure and how? A company invests in the infrastructure and has to be able to make a return on its investment that will cover the capital invested and provide it with a reasonable rate of return.

Any investment will need to make this return over a particular period of time. So, for example, in former days a telecom company would look to make a return on its infrastructure investment in 10-15 years. In more recent times, these investment cycles are much shorter: often companies look to make a full return in five years or sometimes even less.

Often these calculations will not be completely transparent and it will be the regulator's role to clarify with those seeking licences what the expected investment return cycle is. For example, it would be no good the regulator granting a licence for five years when the investment was only to be recouped in the seventh year.

All the models above apply different approaches to making the market deliver high levels of internet use. However, the interests of internet users and private companies are often different, and whilst the market can extend internet access to many people, it is clear that it is not enough on its own. When access is not profitable, it is not provided by the market, and social mechanisms are needed to extend access to the most disadvantaged sectors of society.

9. Access and infrastructure – social models for extending the reach of the internet

Not everyone has access to the internet but in many ways the digital divide is just a prism through which all other inequalities – whether of race, gender, class or whatever – are reflected. The gap in internet access between developed and developing countries is large and continues to grow. Low-income countries account for almost 60% of the world's population but have just under 5% of the world's internet users.

In the developed world, because internet access is fairly widely distributed throughout the population, the digital divide is less acute. Nonetheless governments spend significant sums of money on digital divide initiatives aimed at offering access to poorer people and those in rural areas. Although internet use has grown rapidly from a low base in developing countries (particularly in Africa), this progress is not keeping up with advances in the more developed world. And by their very nature, the governments of low-income countries find it hard to prioritise spending on internet access over more pressing demands like health care.

Because companies providing internet access in low-income countries need to make money (as indeed they do elsewhere), they will target customers who can afford to pay; either middle-class individuals or companies. Obviously there is a relationship between cost of access and the number of users.

Simple economics means that lower costs mean lower access costs and therefore more potential users. The example of the cost of a telephone line illustrates the impact of lowering costs quite clearly. As Dr Ashok Jhunjhunwala, pioneer in affordable telecom solutions, IIT-Madras in India puts it: "It currently costs (an investment of) Rs30,000 to install a single telephone line. To cover this investment, you need a revenue of at least Rs1000 per phone line per month. These rates are affordable to just 2-3% of the Indian population. But if you bring down the investment needed for a phone line to Rs10,000, then affordability of telephones could immediately go up to 30 per cent or more of our population".

The same basic argument holds true for internet costs, which are inextricably linked with telecom costs. The cost of a telephone line is often a key component of overall access costs (see section 6.5). Where telecom companies are government-owned and/or have no competition, the cost of installing new lines is inevitably higher than the costs of lines installed by privately owned companies.

But however much you lower the costs, the market will only provide internet access to those who can afford it. Nevertheless the market can be 'stretched' to provide access to areas that might not otherwise be connected by governments or regulators, by offering continuous or one-off financial incentives. Again these 'market-stretching' initiatives will take internet access out to another layer of people, often paying the capital costs of putting in connections and sometimes subsidising rural call costs.

Beyond the areas that might be served by these approaches lie vast swathes of poor people who do not have the means to buy internet access at all or who cannot afford market prices. For example in Africa, large numbers of its poorest people live widely dispersed across rural areas. Two problems converge: not only are these amongst the poorest people on the planet but they are also spread out and often in physically inaccessible villages. For these areas internet access can only really be delivered if it can be paid for by government or external donors as a social cost. The arguments advanced would be very similar to those advanced for access to telephones.

This has led to a rumbling debate in the development sector about whether the internet is actually a cost effective means of delivering communications benefits to poor people in low-income countries; those living on less than a dollar a day. These are perhaps best summarised in a World Bank paper by Charles Kenny called *The Costs and Benefits of ICTs for Direct Poverty Alleviation.*

In essence the argument is that the internet compares badly in cost terms as a means of reaching people. It is cheaper for an individual to own a radio, and radio broadcasting reaches people more cheaply in their own language. For example, a station in central Mali broadcasts to 92,500 people a year at a cost of just US$ 0.40 cents a person. Likewise a mobile or fixed phone – although more costly than radio – can serve more people at a lower cost than the internet.

The debate has been crystallised by international donors finding that providing internet access (through telecentres) is becoming one more demand on their already stretched resources. For as Kenny puts it, "there is a movement in the development community pushing for widespread rollout of community access points to the internet as a tool for direct poverty relief."

Manuel Castells's recipe for Africa

"As for what to do, in general terms, it is relatively simple... Besides the investment in telecom infrastructure adequate to the needs of developing countries (meaning satellite-based and access by mobile telephony to a large extent, plus open source software with specifically developed applications), there are two key issues. The first is education, particularly of teachers. Since there is no time to proceed in the traditional way, this means mass, virtual education based on the internet. We have the technology, we have the e-learning experience, and there are large institutions...that could be retooled to go from their traditional role as distance education institutions to the new technological medium. Second, the internet is not a gadget but a tool. So the key is to develop and diffuse specific internet-based models for agricultural development, for international, high value-added tourism, for preventative health care, for education, for adult literacy, for citizen information and participation, for community-based security strategies, for horizontal communication and for the diffusion of information, as well as for the diffusion and eventual commercialisation of art and cultural creativity."

Source: *Conversations with Manuel Castells*, 2003, pp. 47-8.

Whether or not you accept this kind of argument, the underlying issue remains one of who pays for the social cost of rolling-out internet access to areas where people have very little money to pay for it. Again, what starts as an internet issue very quickly becomes part of broader discussions about the role of government. Until relatively recently, the telephone company would have been owned by the government and the social priorities of the government of the day would be reflected in what it did. For example, British Telecom was obliged to provide call boxes in a wide range of locations across Britain. Governments would usually cross-subsidise these social costs out of the monopoly profits made from the rest of the operation.

In the world of privatised telecom companies, the role of government shifts. It can no longer do everything, it has to become an 'enabler'. What does this word (much beloved by consultants) actually mean? Well, in this context, it may mean that the government encourages the regulator to set up a universal access fund into which licensed companies pay a contribution, and that these contributions are used to fund rural roll-outs in poor areas.

For example Chile used its universal access scheme to run a reverse subsidy auction in which private companies bid to provide public telephones to un-served areas, the lowest subsidy bid being successful. In a similar fashion, Uganda's regulator has franchised out rural telephony in a particular area and in this instance, the company providing the service will provide a telecentre in one part of the region.

By acting as a facilitator, government can seek to encourage internet take-up in a variety of different ways. E-rate is another example of an approach designed, in this case, to encourage schools to connect to the internet. Started in the USA, e-rate is at its simplest a nationally agreed discounted rate for internet access for schools: often this rate is enshrined in the relevant telecoms legislation at a national level, and therefore is the responsibility of the regulator. Brief descriptions of several schemes give a flavour of what it seeks to achieve:

USA: The US scheme is administered by a not-for-profit organisation that was established by the Schools and Libraries Universal Service Fund. The scheme has six different levels of discount in order to focus the maximum subsidy in poor and rural areas. The method used to measure poverty is the percentage of students eligible for the national school lunch programme that provides a free

lunch to poor students. In its first two years, the e-rate programme connected one million classrooms.

Senegal: The Ministry of Education and Sonatel signed an agreement that establishes preferential terms for access to the internet to make it more affordable to learning institutions. Discounts vary depending on the type of connection but can go as high as 75%. Installation costs are also discounted. Sonatel is directly responsible for invoicing the schools. Sonatel and the Ministry of Education have appointed a co-ordinator for the programme.

South Africa: An amendment to the Telecom Act includes e-rate, which it wants to introduce "to stimulate and facilitate internet usage by public schools. The e-rate will allow public schools a 50% discount on calls to access the internet as well as internet access charges." Although the provision has been made in the Act, implementation of a national scheme has been slow but things are now beginning to move.

The experience of telecentres offers another way providing wider internet access in developing countries. Like cyber cafes they offer the user a chance to connect to the internet without having to buy a PC and often at subsidised rates.

Based on a study carried out Peter Benjamin of the Link Centre in South Africa on telecentres in Africa[1], it is possible to summarise what the experience has been and the costs of providing them. Of the centres surveyed, the average cost of providing a telecentre is up to US$250,000. These projects stress community participation and sustainability, but to date none have proven that they can be self-sustaining without external funding. Most of these centres are supported by foreign donors, though the national programmes for telecentres in South Africa and Egypt can be included in this category.

The Nakaseke Multipurpose Community Telecentres (MCT) in Uganda opened in March 1999. It aims to introduce and test new technologies and applications, and demonstrate the impact of such technologies on development of rural and remote areas. A baseline survey was conducted to establish the nature of information needs of the community and the services. Funding came from international donors (60%), and national government (40%).

The telecentre has eight computers, two printers, a scanner, a photocopier, VCR/TV, video camera and projector. However, frequent power cuts are a problem. As well as phone, fax and internet use, there is a paper and digital library, computer training, and an interesting indigenous knowledge programme where centre staff are building a resource of local health and crop experience.

The centre is just about covering operating costs (subsidised by the community) but there is no expectation that the centre could generate enough income to replace equipment in a few years (depreciation) let alone repay the major capital investment. This centre required great external support (financial and organisational) and so is unlikely to be a model that can become widespread.

The first of the major funded Multipurpose Community Telecentres in Africa was established in Timbuktu in Mali in May 1998. Sotelma, the national telecom was the main local implementer, with other main partners being the ITU, ORTF (TV Mali), UNESCO and IDRC. The majority of the funding of around US$200,000 has come from the external donors. The pilot telecentre is equipped with 11 computers. It offers copying, telephone, fax, and internet services. A major emphasis of the telecentre is to provide training to artisans to set up their web page to sell their handicrafts. The telecentre has proved to be particularly useful to the tour agents organising visits to Timbuktu. The services are subsidised and offered at fees decided by its steering committee.

In Mozambique, two pilot telecentres were established in 1999 in Manhiça and Namaacha (both in Maputo province), funded by the IDRC. They each have four computers, an internet hub and modem, two printers, backup equipment, a public phone, a fax/phone, an external cardphone, a photocopier, overhead projector, whiteboard, TV with video, radio and binder. Current operating costs are just being met by operating income, except for the phone bill. Initial conclusions are that long-term economic sustainability depends on the existence of a critical mass of users and the adoption of computer-related services (over-reliance on phone and photocopy services for income means vulnerability to inevitable future competition and that the major telecentre investment is not justified); technical support, backup and continuous staff training are essential, especially for encouraging the developmental and information services; good communications channels with local authorities and community leaders, and maximum transparency and information regarding the project, are important to success.

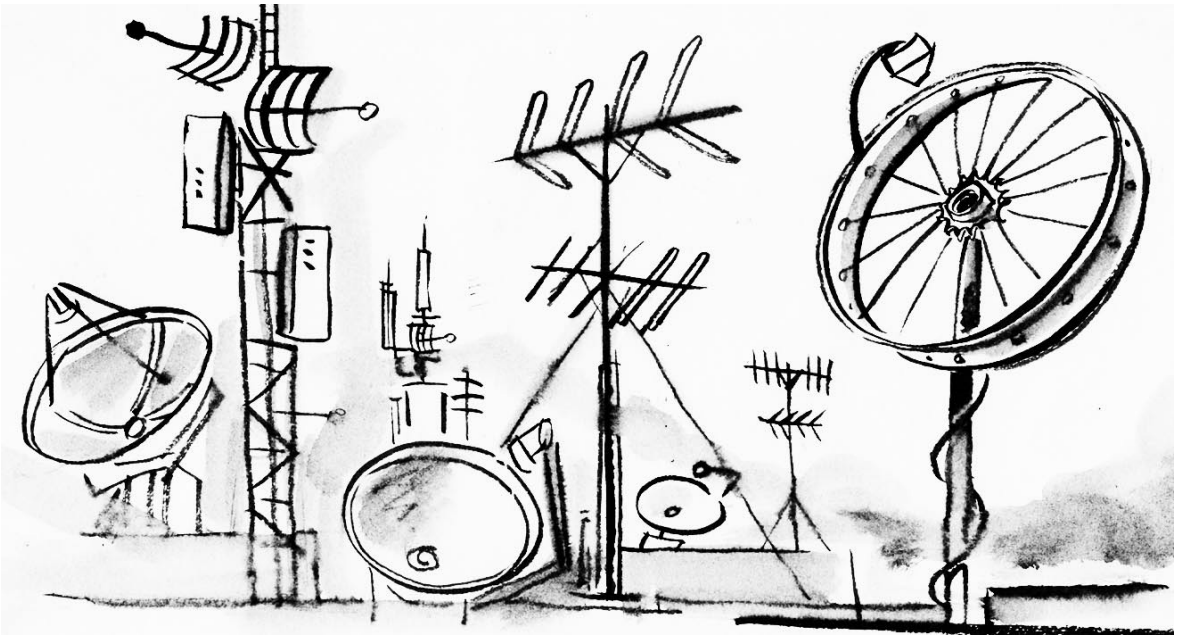
In South Africa, 62 telecentres have been established by the Universal Service Agency. These cost around R200,000 each (US$30,000) and most have four computers, four phone lines, a printer, a copier and TV. Most are in rural areas. Only a few are economically sustainable, mostly through running computer training courses. There have been many technical, financial and managerial problems.

1 See *Balancing Act's News Update* 27 at http://www.balancingact-africa.com

Peter Benjamin's conclusions from the study help define the current limitations of the use of telecentres in low-income areas:

- Centres are managed better where the owners have a stake in them. In some projects, donated equipment is lying around unused. The entrepreneurial instinct is a strong force in making a centre effective.
- There is a great demand for telephony. ICT use can be built, but it takes time, training and local adaptation.
- Simple business models are more likely to be successful than complicated ones. The idea of a multi-purpose telecentre is ambitious. Without extensive training and support, many of the wider aims of telecentres are difficult to reach.
- Computers by themselves are not an information service. Few centres use IT systems to provide information for local use.

A study carried out by Samuel Kyabwe and Richard Kibombo on two villages in Uganda with telecentres showed that internet use among villagers was below 5% compared to 30% for telephone usage and 100% for radio usage.



Rural Internet Access in Dominican Republic

Rural Internet Access is a project of CRESP-EcoPartners at Cornell University and CAREL, the Rural Alternatives Center in El Limon, Dominican Republic. They have operated a wireless rural internet project in El Limon (population 350) for five years, and installed wireless access infrastructure in five additional villages. Internet access for the rural developing world is widely perceived as a way to reduce isolation, provide educational and economic opportunities, and ultimately improve the quality of life. Unfortunately, high capital and operating costs have limited rural access to a handful of heavily subsidised and supported demonstration projects. This innovative integrated strategy, based on existing technologies and rural social structures, addresses a variety of barriers and could ultimately create a breakthrough in getting large numbers of rural communities on the internet. The creation of a strategic demonstration and test bed in four villages in the Dominican Republic is now under way.

Key Elements in this Rural Access Strategy:

- Start from existing clusters of 5-10 villages
- Use wireless networking to share one broadband internet connection
- Maximize the connection's efficiency with a cluster server
- Design an appropriate village computer
- Use open-source software and generic hardware
- Pay for the internet connection by selling voice telephone calls

Source: Rural Intrernet Access Project, http://home.earthlink.net/~jgk5/

Wireless Internet Opportunity for Developing Nations

On 26th June 2003, the Wireless Internet Institute joined forces with the United Nations Information and Communication Technologies Task Force to host "The Wireless Internet Opportunity for Developing Nations" at UN Headquarters in New York City. From the Manifesto of the Conference:

"The prospects of Wireless Internet are by all admissions very promising, offering vast development opportunities worldwide both from a mobility and fixed infrastructure standpoint. Wireless Internet technologies present very attractive opportunities for developing countries to leapfrog several generations of telecommunications infrastructure. Their deployment can become a critical factor in shrinking the digital divide by providing broadband Internet access to whole new segments of underserved populations throughout the world at a fraction of the cost of wired technologies."

Source: http://www.w2i.org/pages/wificonf0603/manifesto.html

National ICT and internet policy and regulation / part 3

National ICT and internet policy and regulation

Government ICT policy is a key item on the ICT agenda today. But not all countries have the same decisions to make, nor the same time frame in which to make them. Whereas most of the OECD countries, for example, have privatised their telecom companies, and have well-established telephone systems that provide internet access to all citizens, in developing countries this is often not the case. Decisions taken in the 1990s in the rich countries, about market liberalisation and deregulation for example, are still being taken in poor countries today. In North America and Europe, how to provide broadband access is a current concern, whereas in Africa most people still do not have access to a telephone, let alone cable TV or satellite connections. Some countries are in the middle – they have initiated their deregulation process, but this is far from complete and de facto monopolies are common.

In this context, a new alignment of international voices has emerged to deal with the big stakes now at play in ICT policy. Powerful intergovernmental organisations are setting the agenda on ICT issues that penetrate all aspects of life – from policy, legislation and regulation to cultural development and the delivery of health and education.[1]

They are working in partnership with the private sector to identify ways to deliver technologies and services to the untapped market of four billion people in developing countries who earn less than $2000 a year and make up the base of the world's economic pyramid.[2]

There is undoubted potential for good in this partnership of development and business. But there are also reservations about the global agenda of liberalisation and privatisation in which it is framed. Externally defined development programmes have rarely succeeded. While national policies do need to take account of the global agenda they must also reflect the knowledge and understanding of local constituents, the needs of the people who will be most affected by the policies and the particular circumstances of their lives.

Civil society voices – national and international - are thus emerging to influence market forces shaping ICT policy towards social equity.

The crucial challenge for the new partnership of development, business and civil society is to turn the digital divide into digital opportunity for those living at the bottom of the economic pyramid. Global development and security demand that the misery that the ITU predicts as an accompaniment to the telecommunications revolution does not add to the burdens of the already poor but that they become the prime beneficiaries of the new opportunities.

This chapter aims to increase understanding of ICT policy and regulatory issues, especially in developing countries, by addressing the following questions:

- What are the objectives of ICT policy?
- How does it link to legislation and regulation?
- Who are the key players nationally and globally?
- Who governs the internet?
- How has telecommunications reform evolved?
- What are the objectives of regulation and how does it work?
- What are key reform and regulatory issues and their consequences?
- What can be done to make decision-making processes more participatory, democratic and transparent?

1 See ITU e-strategy, p. 11

2 CK Prahalad and A Hammond, "Serving the World's Poor, Profitably", *Harvard Business Review*, Reprint R0209C.

10. A short history of telecommunications reform

The year of 1984 was the starting date for the modern history of telecommunications. It saw the introduction of competition into the US market and privatisation in the UK with the divestiture by AT&T of seven regional Bell operating companies (the Baby Bells), the privatisation of British Telecom as a public limited company and the establishment of the British Regulator, Oftel.[3]

The same year also saw the publication of the report of the ITU's Maitland Commission ("The Missing Link"), which firmly established for the first time the link between access to telecommunications and development, and drew attention to the benefits networks could deliver to emergency operations, social services, administration and commerce.

Thus began two decades of parallel and sometimes intersecting work on telecommunications reform and communications for development programmes, culminating in December 2003 with the World Summit on the Information Society[4] held in Geneva. WSIS is a test of whether the telecommunications revolution can meet the twin demands of liberalisation and public service and reconcile the interests of big business, governments and civil society.

Reforms in the telecom sector that emerged in the 1980s responded to the prevailing pro-market climate in many OECD countries. They had a number of negative consequences, including the laying off of workers and inflated returns on investment that led eventually to the burst of the telecom bubble in 2000. They were nevertheless progressively transferred to the developing world through the policy prescriptions formulated by the international development agencies – with the World Bank and WTO in the lead. More and more telecommunications operators came onto the market – the old monopolies, now at least partly in private hands, invested heavily in incumbent operators in developing countries. In an effort to level the playing field for new competitors, new regulatory rules were applied to encourage competition. As competition was introduced into the long distance and international markets the subsidies that had traditionally been transferred from highly priced long distance services to local calls to support universal service were put in question. Regulators introduced new pricing mechanisms to encourage efficient operations and promote competition. Countries were encouraged to build a firewall between governments and regulators.

By early in the third millennium more than 106 telecom operators had been privatised and 110 regulators had been established. The pace of international debate on telecommunications and development had speeded up as well. The collapse of the telecommunications markets in the early years of the new century has not seriously called into question the liberal agenda. In fact the scarcity of investment funds has probably increased the pressure to reform the sector.

3 http://oftel.gov.uk/about/history.htm

4 http://www.itu.int/wsis/

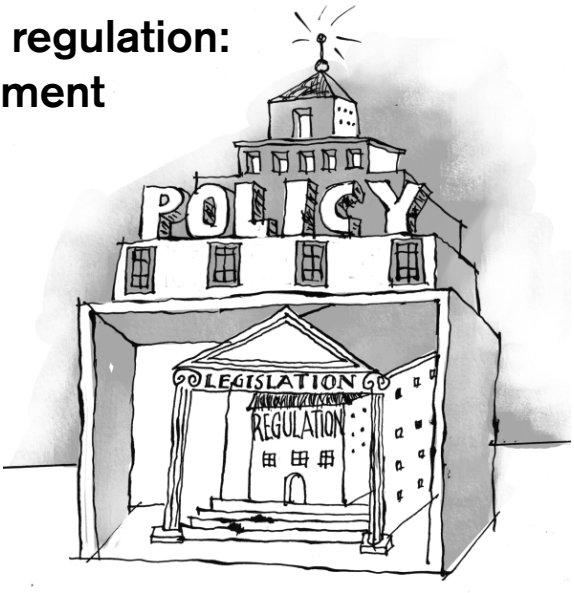
The intersection of telecommunications and development: 1984 - 2003		
Year	Telecommunications[5]	Development
1984	Breakup of AT&T and birth of regional services; privatisation of British Telecom and introduction of price cap regulation; creation of Oftel – the UK regulator	Publication of the *Missing Link* – report of the Maitland Commission highlighting link between telecom and development
1987	1 million cellular subscribers in US and ISDN trials begin	
1988	First transatlantic fibre optic cable completed	
1989	Price cap regulation set for AT&T	
1990	Telmex (Mexico) and Telecom New Zealand privatised	APC was founded
1992		ISOC created
1993	Europe sets 1998 as date for full liberalisation of its telecom market	
1994		ITU Buenos Aires World Telecom Development Conference
1995	25 million cell subscribers in US; 30 million internet users worldwide	G7 Summit Information Society Conference convened in Brussels – pilot projects initiated
1996	Second major AT&T divestiture results in creation of Lucent Technologies; US cell subscribers reach 40 million; Deutsche Telekom is privatised; US Telecom Act opens competition to all markets provided that the companies met certain pro-competition requirements	Information Society and Development Conference convened by EU and South Africa in Johannesburg
1997		Global Knowledge for Development Conference convened in Toronto by consortium of development organisations
1998	WTO Agreement on Trade in Basic Telecom Services	ICANN created
2000	Y2K passes without disaster; mergers abound; Clinton calls for increase in universal service fund to accommodate native American reservations and their technology needs; the telecom market begins to weaken	Second Global Knowledge for Development Conference convened in Kuala Lumpur; G8 Okinawa Declaration calls for action to exploit development potential of ICTs; UN puts the information society on its agenda through discussions at ECOSOC its high level economic and social council; UN Millennium Assembly calls for partnership to promote ICT for development
2001	Markets continue to fall – corporate governance called into question; cell phones in Africa (25,352,900) outnumber fixed line phones[6]	The UN ICT Task Force created to advise the Secretary General – experts from all sectors – APC represented
2002	More than 106 incumbent telecom operators have been privatised; 110 regulators have been established[7]; cell phones in Asia (440,260,100) outnumber fixed line phones	Regional and global meetings convened to prepare for World Summit on Information Society
		Source: ITU, *Asia Pacific Telecommunication Indicators*, 2002.

5 http://webbconsult.com/1980.html

6 http://www.itu.int/ITU-D/ict/statistics/at_glance/cellular01.pdf

7 ITU, *Effective Regulation: Trends in Telecommunications Reform* 2002, p. 21.

11. ICT policy, legislation and regulation: tools for national development



From policy to legislation and regulation

Policy is the key determinant of legislation and regulation. It sets out the vision for ICT and its links to national development goals. Legislation establishes how policy is implemented by providing the statutory foundation for the required institutions (for example, consultative, advisory and regulatory bodies) and processes (for example, licensing).

Legislation specifies the financial, staffing and reporting regimes under which the regulator operates and which define its functions and degree of independence. Regulatory agencies are responsible for developing regulations that lead to the implementation of policy and policy objectives, such as, for example, new tariff structures and universal access programs.

Process	Example
Policy (the vision)	The Ministry of Communications develops a new national policy aiming at establishing a liberalised telecom environment, opening telecom markets to competition (for example, long distance and basic services)
Legislation	A new telecom Act is passed establishing the new regulator as an independent government agency and establishing target dates for opening each market to competition
Regulation	The regulatory agency implements a new tariff structure (slowly eliminating cross-subsidies among long-distance and local services) and starts the process to license new operators

The broad objectives of policy

The main objective of national ICT policy is to balance the benefits and the risks of expanded ICT use in a way that is consistent with national development goals. Generally, this broad goal translates into a number of specific policy choices:

- What to privatise? And when?
- When to introduce competition in each market?
- When to introduce regulation?
- What to regulate and what to leave to market mechanisms?

These choices will be explored further in chapter 16.

The scope of policy

While policies must address the extension of the communications infrastructure through telecommunications reform to stimulate private sector growth and create job opportunities, this is a necessary but by no means sufficient condition for an effective ICT contribution to national development goals. ICT policy must also incorporate social goals by building human capacity and creating the conditions for the development of relevant applications and content.

ICT policies have to do with education, health, agriculture, culture and all other areas of activity that impact on quality of life. They can be integrated into sectoral as well as broad national policies; for example countries may commit to introducing ICTs into schools in order to expand educational opportunities and increase the supply of ICT-literate graduates; they may extend internet access to rural clinics to improve the delivery of health services. As the use of the internet expands within countries a host of specific issues emerge: privacy and security, intellectual property rights, access to government information are examples.

E-Sri Lanka is a vision that will help heal the divisions of the past

Sri Lanka has captured a window of opportunity to harness the ongoing information and communication technology revolution in support of enduring peace, accelerated growth and fair equity. The e-Sri Lanka miracle has become a model of an ICT-enabled development strategy whereby information technology is exploited for broad-based growth involving all key sectors of the economy and society.

http://www.esrilanka.lk/roadmap.htm

An example from Mauritius

The Mauritius government began the reform of its telecommunications sector in 1997 with the publication of a discussion paper (Green Paper); following extensive consultation the policy (White Paper) was published; a new **Telecommunications Act** was passed in 1998.

The Policy of the Republic of Mauritius with respect to the telecommunication sector establishes a vision:
"To develop Mauritius into a modern nation and to enhance the nation's competitiveness in the global market place so as to improve the quality of life of the people…"

Including a set of principles to govern development of the sector:

- The active promotion by government of an information-based economy;
- The promotion of competition and network interconnection as circumstances permit;
- An effective and independent regulatory body with clearly defined powers and responsibilities;
- Private sector participation to the greatest extent possible;
- The termination of all exclusivity provisions by the end of 2004. [1]

The regulator – the Information and Communication Technologies Authority – was established by the Information and Communication Technologies Bill which identified its objectives, structure, powers and functions. The bill also created advisory and dispute settlement mechanisms.

The Mauritius legislation addresses both economic and social goals through the creation of a telecommunications regulatory authority as well as a national advisory body and appeals board. It aims to democratise access to ICTs and at the same time increase competition and link Mauritius firmly to the global information economy.

Mauritius' information and communication technologies bill (No. 38 of 2001)

Explanatory Memorandum

The object of the above Bill is to provide for –

(a) the establishment and management of an Information and Communication Technologies Authority;

(b) the regulation of the information and communication technologies sector including -

- telecommunications;

- the use of the Internet;

- the enhanced development of an information society and online services;

- the protection and security of data;

- the facilitation of convergence; and

- the establishment of ICT Advisory Council and of an ICT Appeal Tribunal

(c) the democratisation of information and communication technologies for the promotion of a knowledge-based society.

(d) the transition towards a fully liberalised and competitive market in the information and communication sector.[2]

The legislation sets out the structure, objectives, powers, functions and tools of the regulator, in this case the Information and Communication Technologies Authority. The legislation makes provision for the creation of an Internet Management Committee, which, *inter alia*, is responsible for organising stakeholder input into discussions related to the internet and for advising the Authority on internet issues. It is the responsibility of the regulator to implement the policies detailed in the legislation. Chapter 15 looks more closely at the nature of regulation.

1 http://ncb.intnet.mu/mitt/ministry/policytel.htm

2 http://www.icta.mu

12. Involving key players at the national level

Who determines ICT policy?

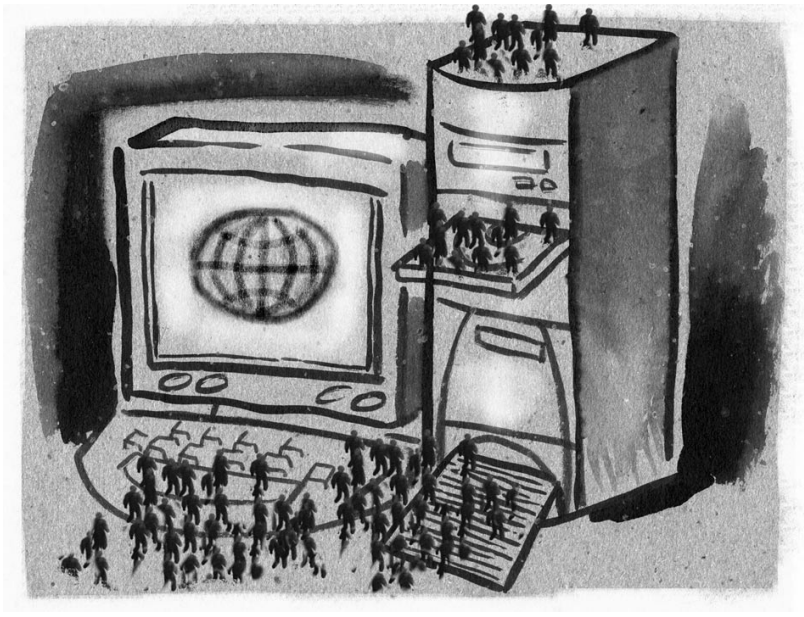
Broadly speaking there are three groups of national stakeholders: government and other public sector bodies; civil society; and the private sector. All play a role in national ICT policy-making.

The Office of the Prime Minister or the President, the Ministry responsible for communications, other ministries relying on communications facilities to deliver their programmes, the telecommunications operators (if they are still publicly owned), the regulator (if it has already been established) are all part of the government constituency.

Interested civil society organisations include non-governmental organisations promoting the internet, trade unions, community development organisations, professional associations, forums of ICT users.

The private sector ranges from single entrepreneurs setting up small ICT businesses to the big multinationals active in the country (internet service providers, software developers, technology producers, telecoms providers) and includes businesses that are users of technology, industry groups, chambers of commerce.

Negotiations should aim at a consensus among the three sectors on appropriate ICT policy; all share responsibility for ensuring that policy is carried through in legislation and regulation and for monitoring the implementation of the policy once the regulatory institutions have been established.



Governments

Government is usually the driver of ICT policy development. Key players from the public sector are the Ministry responsible for communications, the national telecommunications operator and the regulator. Other ministries with an interest in the outcome should also be involved. These include, for example, education, health, trade and industry.

The importance of broad-based, high level leadership

Leading the policy reform process from the office of either the President or the Prime Minister – as was the case in Mozambique – has advantages: it demonstrates high level commitment to ICT policy, it ensures that the process is not captured by the narrow technical concerns of the communications sector and it ensures that all interested ministries and public sector bodies will be encouraged to participate.

Civil society actors

The success of policy depends on how people use the new tools that become available to them – computers, fixed line phones, mobiles or the internet – once the policy is implemented. It is trite but true to say that the chances for them to use the tools successfully to meet their own needs will be increased if they have a say in defining how the tools are delivered. Civil society organisations are one key link (parliamentarians are another) between the broad population and policy processes. They have unique experiences and values to contribute regarding the use of the tools for social objectives.

Is there evidence of civil society involvement?

Open consultations in public meetings held throughout the country, and interactive web sites that provide space for comments and access to relevant documents, are used widely in the North to ensure public participation in both policy and regulation. This is the case in Canada, for example, both for internet policy development (http://connect.ca) and for telecommunications (http://www.crtc.gc.ca).

It is more of a challenge to organise civil society participation in developing countries where the habits of consultation may be less entrenched, organisational structures less developed and communication of all kinds more difficult.

In Mozambique, telephone and internet use is limited outside the capital and a few provincial towns. The govern-

ment is, however, championing ICT as a tool for development throughout the country. During the course of policy development the Information Policy Commission organised a series of public meetings in the provinces to engage local groups as its work progressed.[1]

The Indian government, following the recommendation of its National Task Force on Information Technology and Software Development, encouraged each state government to develop an IT policy. In this case the state-level polices appear to have been defined largely by the government and private sector.[2]

The experience in Africa

The Association for Progressive Communications (APC) commissioned a series of studies on the involvement of civil society in the development of ICT policy in Africa.[3] The studies cover Benin, Cameroon, Egypt, Ethiopia, Kenya and Senegal. They provide a good starting point for understanding the role that civil society organisations can play in shaping ICT policy – and the challenges they face.

Senegal

Senegalese civil society has very little involvement in the formulation and application of

ICT policies, for the following reasons:

- Owing to its lack of internal organisation, civil society is not recognised as a representative participant by the authorities responsible for defining ICT policies.
- The organisation of civil society on an institutionally representative basis could be difficult, moreover, because of the wide range of interests it covers.
- There is still only a limited number of CSOs with direct involvement in ICT issues (development NGOs), and the number of partners who could potentially participate in ICT policies is even smaller.
- CSOs that could be more immediately involved in the area of ICT policies mainly comprise persons who are professionally involved in ICT, and come from the social sectors (public, private, educational, CSOs).

Source: *APC Africa ICT Policy Monitor*, http://www.apc.org/english/rights/africa/research.shtml

Kenya

Civil society has played a significant role in the development of ICTs by creating awareness, and training by introduction of services in the early 1990s. Apart from the supply of email services, civil society lobbied for an improved policy and regulatory framework. Today, civil society has shifted its focus to higher values to guarantee access to information as a human right. Additionally, civil society is using internet for development and empowerment. The challenges that remain are low penetration, lack of content and economic barriers.

Source: *APC Africa ICT Policy Monitor*, http://www.apc.org/english/rights/africa/research.shtml

Some successes

There are success stories. In Cameroon, perhaps partly because government leadership on information society issues was fragmented among different ministries, civil society organisations with a history of ICT work were able to establish themselves as important credible interlocutors of government in spite of its normally secretive way of doing business. In Egypt, civil society was instrumental in ensuring recognition of the legal right to privacy in the recently adopted Communications Bill.

In general, however, civil society participation has been ad hoc and often delivered through individual experts rather than through representative voices of civil society groups. Often there are no channels available for CS participation. In Spain, for example, a large campaign was built up in the internet against the government's new internet bill, but it made little impact outside the restricted circles of internet users. So while it is the case that there is almost universal acceptance of the principle that information policy will only be an effective instrument if it is developed by all stakeholders including civil society, work still needs to be done to strengthen the instruments which will guarantee that civil society is present and listened to.

Proposals emerged to reinforce civil society's role in ICT policy processes by:

- Exploiting international links: international organisations as divergent as APC and the World Bank today agree on the need for civil society participation in policy and strategy development
- Organising the ICT civil society sector internally through the establishment of a national ICT forum – competition between organisations hampered effective communication in a number of the countries studied
- Linkage with CSOs with broader development goals in order to build awareness of ICTs and provide appropriate training to help CSOs use ICTs effectively

1 http://www.infopol.gov.mz

2 R Mitra, *Emerging State Level ICT Development Strategies*, Chapter 16 at http:// www.worldbank.org/wbi/documents/sn37160/Chapter16-17-Bibliography.pdf Chapter 16

3 http://africa.rights.apc.org

- Increasing understanding of government processes, lobbying and public relations.

Anti-democratic internet administration is tackled in Brazil

In Brazil civil society recognised early the potential of the internet. Training, awareness-raising and lobbying with NGOs has created a critical mass of users, which is now empowered to tackle ICT policy issues including internet management and rights.

In January 2003, at the World Social Forum in Brazil, APC representatives criticised the anti-democratic nature of internet administration. Prominent Brazilian ICT activists complained that the management of the Brazilian internet was in the hands of a group of volunteers who are appointed by the Brazilian ministries and yet work behind closed doors, with no accountability for the millions of dollars raised in the sale of .br internet addresses.

Brazilian civil society got together to change the way the internet is governed in Brazil. A seminar was held on 25-26th February 2003 in Rio de Janeiro and, partly as a result of discussions with government officials and the seminar recommendations, the Lula government decided to support the transition to a new internet governance structure for Brazil. It was proposed that profits from the sale of .br addresses go to create a new digital inclusion fund.

Source: *APCNews/RITS*, http://www.apc.org/english/news/index.shtml?x=12139

The private sector

Computing, communication and media businesses – large and small - all have a stake in the policies that govern the ICT sector.

Import duties on hardware and software, the restructuring of the telecommunications sector to allow for competition by fixed-line, and mobile operators and the concentration of ownership of radio, television and the print media, are examples of the kinds of issues of concern to business as well as consumers.

The ICT private sector in the North is generally well organised but in developing countries it may face many of the same challenges as civil society in trying to organise and develop positions that can impact on policy processes. It can engage government systematically on ICT issues only if it is itself organised into interest groups. For example, the internet service providers in South Africa acted individually throughout the telecommunications reform process that took place in the mid-1990s. ISPs realized the benefits that could accrue from forming an association to develop and lobby for joint positions. The creation of the ISPA (Internet Service Providers Association) has enabled much more effective input from ISPs into subsequent South African ICT policy processes.

Internet strike in Europe

Civil Society actions on national ICT policy decisions about access are not limited to developing countries. For example, in 1999, thousands of Internet users in at least three European countries, France, Germany and Spain, staged an Internet strike in protest over the high cost of dialup access. They refused to connect during 24 hours, to pressure their governments into forcing the telephone companies to allow a flat rate telephone call charge for Internet access, rather than the cost per minute that is normal now.

Source: Asociacion de Internautas, http://www.internautas.org/NOTICIAS/ENE99/28.htm

Participatory policy making in Nepal: An example of successful policy partnership

Participation is a highly effective strategy for rallying key people behind public policy. This is what Dr Ramesh Ananda Vaidya, Chairman, Information Strategy Formulation Steering Committee, National Planning Commission discovered when he opted for a participatory approach towards formulating a policy for Nepal's information technology sector. It is one of the first instances when such an approach has been attempted in making national policy in the country.

…we adopted a participatory process in which the government, private sector and civil society share a common discussion forum during policy design. We believed such a process based on the consensus of IT stakeholders would lead to a 'global congruence' among them and thus facilitate successful development of the IT sector.

The year long policy design process was launched with a series of informal consultations with members of the IT industry. This led to the creation of a Steering Committee composed of three members of the government, a member of the private sector, the Vice-Chancellor of Tribhuvan University, the Executive Chairman of the Institute for Integrated Development Studies and two members of the International Centre for Integrated Mountain Development.

A series of strategy papers was prepared and presented to a National Stakeholders Workshop held in Kathmandu. Participants represented a diversity of groups including gender specialists, development workers, Internet Service Providers, journalists.

The workshop – and comments received via e-mail - generated valuable input into finalizing the policy which was approved by government in October 2000.

Source: PAN Asia, http://www.panasia.org.sg/news/rnd_st/ict_rnd04a.htm

13. The actors in international and regional internet and ICT policy

The alignment of international opinion

Many international forces come into play when countries begin to define the policies that shape the new technologies and the internet to their own development goals:

The **international organisations** that define the global information economy and the rules under which countries can connect to it – as well as the conditions under which support will be available for the implementation of ICT programmes. Key among these are the International Telecommunications Union, the World Intellectual Property Organisation, the World Trade Organisation, the World Bank and the World Economic Forum.

International non-governmental organisations promote alternative visions of globalisation and work to ensure a role for civil society in shaping the information society globally, regionally and nationally. This is a growing and increasingly influential family of organisations of which we can only cite a few examples here, such as the APC and the APC-WNSP, Panos, and Bridges.org.

Regional organisations which may play a promotional role and enhance collaboration; the Economic Commission for Africa with its African Information Society Initiative and the regional development banks are examples.

The organisations that govern the internet: The Internet Society, the Internet Engineering Task Force, the World Wide Web Consortium and the Internet Corporation for Assigned Names and Numbers (see chapter 14).

13.1. International organisations: the mainstream position

Five organisations dominate mainstream dialogue on global ICT policy issues:

- The International Telecommunications Union because of its mandate for telecommunications within the United Nations system
- The World Intellectual Property Organisation because it is responsible for setting the rules that govern ownership of content on the internet
- The World Trade Organisation because it sets the rules for international trade
- The World Bank because of the financial and technical resources it brings to bear on development, and
- The World Economic Forum because of its ability to convene the world's rich and powerful.

The World Bank, WTO and WEF have been subjected to extensive criticism over the last decade because of the role they have played in promoting a global liberalisation agenda which has reinforced the digital divide and further marginalised poor people and poor countries.

International Telecommunications Union (ITU)

ITU is the specialised agency within the United Nations System where 189 governments and over 600 private sector members coordinate global telecom networks and services (www.itu.org).

Founded on the principle of international cooperation between government and the private sector, the ITU is the global forum through which government and industry can work towards consensus on a wide range of issues affecting the future direction of this industry.[1] The changes in the telecommunications industry, where privatisation has meant that the private sector has become dominant and government telecoms no longer have the same importance as in the past, have meant that the ITU has adapted to the times and become more responsive to private companies. Companies both large and small can become members of ITU sectors by paying membership fees, and companies provide much of the technical input to the decision-making process. Lower fees are available for membership in the Telecommunications Development Sector – in particular for members from developing coun-

1 http://www.itu.int/members/index.html

tries. Civil society has historically been a neglected partner but is increasingly present today through participation in national delegations or through being granted an observer status.

ITU's mission covers technical, developmental and policy issues.[2] Much of its authority derives from its World Conferences, which review, revise and adopt the regulations that form the framework for the provision of international telecommunications services.

It also establishes the technical characteristics and operational procedures for wireless services, manages the global radio frequency spectrum and coordinates international standard setting activities including standards for Internet Protocol (IP) networks and IP-based systems.

Its Development Sector implements communications development projects that are funded by the UN and other sources, and publishes definitive information on telecommunications trends.[3]

The ITU Strategy

The ITU's e-strategy shows how far it has moved from its technical mandate into areas of broad public concern. Its goals are to:

- Foster the development of Internet Protocol (IP) networks and services on all types of telecommunications networks
- Integrate the development of IP with societal applications to enhance governmental, medical/ health, educational, agricultural, business and community services
- Enhance security and build confidence in the use of public networks
- Continue the development of Multi-purpose community telecentres (MCTs) and multipurpose platforms (MPPs) as a mechanism to provide wider and affordable access to ICTs
- Enhance ICT literacy and increase public awareness of the potential of ICTs for socio-economic development
- Promote the establishment of a favourable legal environment for e-applications
- In all applications, take into account the needs of rural, isolated and poorly served areas and people with special needs (women, youth and indigenous people).

Source: ITU, http://www.itu.int/ITU-D/e-strategy/

2 This section draws on H Intven (ed) *The Telecommunications Regulation Handbook*, World Bank, 2001.

3 Two key sources of information are the *World Telecommunications Development Report* and *Trends in Telecommunications Reform* published regularly by ITU.

World Intellectual Property Organization(WIPO)

WIPO is a specialised agency of the United Nations responsible for promoting the protection of intellectual property worldwide. 179 countries are WIPO members; national and international non-governmental organisations may apply for observer status (www.wipo.org).

WIPO is responsible for administering 23 treaties in the field of intellectual property. The treaties define internationally-agreed basic standards of protection in each country, provide facilities to ensure that international registration or filing is valid across national boundaries and create a universally agreed classification of intellectual property to ease searching and information retrieval.

The ICT revolution has probably had a greater impact on WIPO than on any other UN agency. Intellectual property rights in the past were fundamentally territorial in nature and defined by national governments. The internet is a quintessentially global medium and the home of much of today's production of intellectual property. WIPO faces large challenges in leading the way towards a system of intellectual property rights that recognises the global information society and can adapt to its changing dimensions.

World Trade Organization (WTO)

The WTO is an international agency that deals with the global rules of trade between nations; telecommunications and internet services have taken on increased importance within its trade agenda.

Its membership (standing at over 130 countries accounting for over 90 percent of world trade) is at the level of governments. Its day-to-day business is conducted by the General Council, which is composed of representatives of all WTO members (http://www.wto.org).

The WTO administers trade agreements, supports negotiations, rules on trade disputes, and assists developing countries on trade policy issues through technical assistance and training.

The WTO has become the most influential institution within the global telecommunications market. It is responsible for the administration of the General Agreement on Trade in Services (GATS), its Annex on Telecommunications and a Protocol on basic telecommunications services known as the Agreement on Basic Telecommunications (ABT). As well as dealing with the liberalisation of telecommunications services and tariff-free trade in information technology products, it addresses intellectual property rights and e-commerce, issues that are key to the development of the information society.

GATS and ABT are the instruments that have pried open the global telecommunications market. Countries are not all required to pursue the same pace of liberalisation but, once signed, the obligations and disciplines the agreements contain become binding and initiate a process from which there is no return.[4]

The World Bank Group

The World Bank Group plays a major role in defining the global agenda for development. It has been instrumental in identifying progress towards market liberalisation as a key determinant of development. It has also led efforts to link national ICT policies with poverty reduction strategies as a means of promoting progress towards the UN's Millennium Development Goals (MDGs)[5] . These positions are not necessarily easy to reconcile and result in lending programmes with conditions that may prove difficult for countries to meet.

The WB also has access to extensive technical resources, which allow it to develop definitive positions on the regulatory and technical issues involved in ICT and internet policy and programme development.

The World Bank is governed by a Board, which includes all its members; it is important to know that decisions are taken by majority vote with voting rights determined by the number of stocks held in the Bank. Twelve Executive Directors are responsible for the conduct and operations of the Bank. Five of them are appointed by the five member governments with the largest number of shares.[6] The WB is inevitably therefore controlled by the rich countries, which hold the major part of the voting shares, in particular the USA.

The Group's Global Information and Communication Technologies Department (GICT) combines the private sector investment capabilities of the IFC with the public-sector advisory and financing expertise of the WB, and a global donor-funded program infoDev.[7]

As with the ITU, the GICT Strategy[8] is moving beyond a technical focus on privatisation, liberalisation and infrastructure and towards applications that promote equity and reduce poverty. It will put increased emphasis on e-governance, e-commerce and other sectoral applications through new financing mechanisms and technical assistance grants.

The World Economic Forum (WEF)

The World Economic Forum is a private organisation that provides a collaborative framework for world leaders to address global issues and promotes entrepreneurship in the global public interest. It is funded by fees from the 1,000 foremost global companies and works in partnership with other organisations including labour, media and NGOs.[9]

ICTs are integrated within its Global Competitiveness Programme; its annual Global Information Technologies Report provides a comprehensive assessment of networked readiness covering most of the leading economies of the world.[10]

The WEF's convening power makes it an influential voice in the establishment of global policies on ICT issues; its competitiveness and IT reports are used by businesses and development agencies to help target investments in IT infrastructure and technology and grant funding for ICT development initiatives.

13.2. International NGOs: developing an alternative vision

Civil society is developing its own powerful voices to balance the more entrenched authority of the organisations described above. The Association for Progressive Communications is the premier organisation articulating civil society's position on ICT policy issues but it is increasingly strengthened by the recognition that related international NGOs are giving to ICT issues. Those mentioned below are only a few examples of the organisations that are adding weight to alternative visions of the global information society.

The Association for Progressive Communication (APC)

The APC is a non-profit association of member and partner networks around the world, committed to making the internet serve the needs of global civil society.[11]

APC has developed a number of tools to build capacity within civil society to address ICT policy issues and ensure that its views are heard in global debate.

---

4 T James (ed), *An Information Policy Handbook for Southern Africa*, IDRC, 2001, p. 7

5 http://millenniumindicators.un.org/unsd/mi/mi_goals.asp

6 http:// web.worldbank.org http://web.worldbank.org/WBSITE/EXTERNAL/EXTABOUTUS

7 http://info.worldbank.org/ict/

8 http://info.worldbank.org/ict/ICT_ssp.html

9 http://www.weforum.org/site/homepublic.nsf/

10 S Dutta, B Lanvin and F Paua (eds), *Global Information Technologies Report 2002/2003, Readiness for the Networked World*, Oxford University Press, 2003.

11 RLINK http://www.apc.org

The APC Internet Rights Charter highlights some of the specific issues that individuals, civil society organisations, community media, and policy makers and regulators, need to consider in their efforts to protect the right to communicate freely via the internet and realise its potential to create a better informed and more just world.

The ICT Policy Monitor Websites for Latin America and the Caribbean, Africa and Europe signal critical developments that threaten or promote internet rights.

The APC-WNSP trains women and gender advocates on ICT policy from a gender perspective and is actively involved in ensuring that gender is integrated in ICT policy.[12]

APC provides support for several campaigns, such as the Communications Rights in the Information Society (CRIS) launched by the Platform for Communications Rights to ensure that rights are high on the agenda of all who deal with ICT policy – and in particular that they receive full consideration by the World Summit on the Information Society.[13]

Training programs and research help CSOs understand how ICT policy decisions can affect their work.[14]

PANOS is a global network working with journalists in developing countries to report on and analyse key issues of the day – including ICT and development. It has recently undertaken, with the Commonwealth Telecommunications Organization, a survey of factors inhibiting developing countries from participating in ICT policy-making, and recommended actions to overcome them, which are discussed in section 3.8. / (www.panos.org.uk).

BRIDGES.ORG is an international non-profit organisation working at the interface of international policy and cutting edge technologies, *inter alia* through the provision of advice to ICT policy makers and support for projects that demonstrate the use of ICTs (www.bridges.org).

GIPI– the Global Internet Policy Initiative – serves as a resource to local stakeholders in the internet policy development process. The project's goal is to promote: transparency and predictability in business regulation; competition, privatisation, open networks and universal service in terms of telecom policy; and market-driven solutions, user-control and human rights protection in terms of government control. The key people in GIPI are the country coordinators who help local stakeholders to develop the capacity to promote sound policies supporting an open internet (www.gipiproject.org).

CPSR– Computer Professionals for Social Responsibility – is a public-interest alliance of computer scientists and others concerned about the impact of computer technology on society. It works to influence decisions regarding the development and use of computers, which have far-reaching consequences. CPSR members provide the public and policy-makers with realistic assessments of the power, promise, and limitations of computer technology and direct public attention to critical choices concerning the applications of computing and how those choices affect society. / (www.cpsr.org).

EFF – the Electronic Frontier Foundation – is a pioneering donor-supported membership organisation working to protect fundamental rights regardless of technology; to educate the press, policy-makers and the general public about civil liberties issues related to technology; and to act as a defender of those liberties. Among its various activities, EFF opposes misguided legislation, initiates and defends court cases preserving individuals' rights, launches global public campaigns, introduces leading edge proposals and papers, hosts frequent educational events, engages the press regularly, and publishes a comprehensive archive of digital civil liberties information (www.eff.org).

12 http://www.genderit.org

13 http://www.crisinfo.org

14 http://rights.apc.org

13.3. Regional organisations: promoting regional positions

Many regional and sub-regional organisations with a development mandate have staked out roles with respect to information society, ICT or internet policy.

The European Union has developed the concept of Europe as part of its strategy to grow a knowledge-based economy and increase employment and social cohesion. The eEurope framework is guiding the e-strategies of countries that are candidates for EU membership. Several EU Directives on ICT and the internet have had an influence far and beyond the EU member countries.[15]

The **African, Asian and Inter-American Development Banks**[16] provide financial and technical assistance for the establishment, expansion, improvement and integration of public telecommunications systems. Expanding access to telecommunications services, improving the contribution of the telecommunications sector to economic growth, and improving competitiveness of the sector through privatisation are issues on the agendas of the Banks.

The **African Telecommunications Union** (ATU) provides a forum for African governments, as well as public, private and social sector organisations involved in ICT, to formulate policies and strategies aimed at improving access to information infrastructure and promoting its use as a tool for stimulating economic development and enhancing poverty reduction.[17]

The **United Nations Economic Commission for Africa** (UNECA), within its African Information Society Initiative, provides advice on information policy to member states, stimulates regional debate, and promotes Africa's voice within global debate.

The **Latin American Forum of Telecommunications Regulators** (REGULATEL[18]), and the **Telecommunications Regulators Association of Southern Africa** (TRASA[19]) encourage coordination among regulatory authorities in their regions and promote the exchange of experience and ideas on telecommunications policy and reform.

Regional Common Markets (such as Mercosur for southern Latin America and COMESA for East and southern Africa) also have interests in implementing policies and standards that move in the direction of integrated telecommunications markets within their regions.

13.4. Private enterprise

We should not forget that the private sector plays a key role in setting ICT policy. This may be through:

- Direct or indirect influence in organisations such as the ITU or the WTO
- Participation in technical standards bodies for the internet
- Employers federations or even individual companies which lobby or put pressure on governments or international organisations to respond to the demands of this sector
- Actions in the courts to enforce existing laws or to create precedents.

15 guesten.ksh?p_action.gettxt=gt&doc=IP/03/1005|0|RAPID&lg=EN&display=; cf also http://www.ipjustice.org/ipenforcewhitepaper.shtml

16 http://www.afdb.org, http://www.iadb.org, http://www.adb.org

17 http://www.atu-uat.org

18 http://www.regulatel.org

19 http://www.trasa.org

14. Guiding and governing the internet

Emerging as it did from the US defence establishment – and depending for its development on highly technical skills – it is not surprising that the internet was governed for years by a small group of relatively invisible men. Today decisions taken on internet standards have political, economic and social ramifications as well as technical ones. Governments, business and civil society organisations alike recognise that internet decisions carry high stakes. Opening up decision-making processes is imperative.

Four organisations have particular roles to play:

- The **Internet Society (ISOC)** is an open, inclusive global internet movement
- The **Internet Corporation for Assigned Names and Numbers (ICANN)** is the most controversial, because its responsibility for managing domain names globally touches national sovereignty and calls for broader participation in decision-making
- The **Internet Engineering Task Force (IETF)** looks after standards for internet connectivity
- The **World Wide Web Consortium (W3C)** looks after standards for accessing web-based content.

The **Internet Society (ISOC)** is a professional membership society with 14,000 individual members and 150 organisational members in over 180 countries. It provides leadership in addressing issues related to the future of the internet. It fosters an environment of international collaboration within which to support the development of standards, create educational and training opportunities and promote professional development and leadership.

Members are the **companies, government agencies, and foundations** that have created the internet and its technologies as well as innovative and entrepreneurial organizations contributing to the maintenance of that dynamic.[1]

Membership is free to individuals; organisations pay between US$2,500 and US$100,000 annually. Fees for non-governmental organisations are discounted by 50%. Members can work through local chapters – or create them when none exist.

The **Internet Corporation for Assigned Names and Numbers (ICANN)** is a global, non-profit, private sector initiative that was formed when the USA realised that management of the domain name system from a narrow, technocratic base was no longer feasible. ICANN's main function is to coordinate the assignment of domain names, Internet Protocol addresses, protocol parameters, and port numbers that must be unique in order to achieve a functioning, secure and stable internet.

ICANN has no statutory or other governmental power – its authority derives entirely from voluntary contract and compliance with its consensus policies by the global internet community.[2] Its survival depends on reinventing itself in a more truly global mode.

As a result of lobbying by a number of civil society bodies the ICANN Board opened up its membership to on-line election by individual members 'at large', who registered on-line; they were entitled to vote in the last Board election. Five members were elected under this new arrangement. The elections have proved controversial within the ICANN Board and within the broader internet constituency; rules have been changed so that the 'at large' community of individual users can no longer vote in ICANN Board elections. [3] Some alternative ways of expanding participation in ICANN are discussed in chapter 17.

The **Internet Engineering Task Force (IETF)** is a network of individuals hosted by ISOC and engaged in the development of new internet standard specifications. It is the ultimate consultative mechanism of the internet age. It has no corporate identity, board of directors, members or dues.[4] It deals nevertheless with the pressing operational and technical problems by specifying standards or protocols; it moves technology innovations from its research group to the broader internet community; and it acts as a forum for the exchange of information between vendors, users, researchers, contractors and network managers.

1 http://www.isoc.org/isoc/

2 http://icann.org

3 S Reddy, "Can ICANN meet the needs of less developed countries?" May 20, 2003, http://www.circleid.com/articles/2595.asp,

4 http://www.ietf.org

The **World Wide Web Consortium (W3C)** was created to realise the full potential of the Web by promoting interoperability and encouraging an open forum for discussion.[5] It groups 74 people working from locations around the world and is hosted in the USA, France and Japan. W3C has a truly global vision of a web that accommodates differences and limitations across continents, is user-friendly and trustworthy. It aims to match the web to the ever-changing expectations of users and the ever-expanding power of computers. In a recent battle over patenting web standards, the Consortium demonstrated a willingness to listen to free software voices within civil society and came down firmly in support of a Web maintained clearly within the public domain, and gave an example of how to respond to civil society pressure that other such bodies could follow.[6]

5 http://www.w3c.org

6 http://www.w3.org/Consortium/Patent-Policy-20030520.html, http://www.redhat.com/advice/speaks_w3c_patent.html

15. Telecommunications regulation

Three basic ingredients appear in most reform programmes – private sector participation, market competition and the creation of an independent regulator. The interpretation and sequencing of these ingredients within the overall mix of policies is what distinguishes one approach from another, and may be as important to successful reform as the individual ingredients themselves.[1]

The new ICT environment – privatised, competitive, responsive to fast paced technological change and convergence – shapes regulatory requirements. Three broad groups of converging activities are subject to regulation within the sector: telecommunications, broadcasting and the internet. Regulation of these sectors is increasingly concentrated in the hands of a single agency. Market mechanisms now play a greater role in setting prices that were regulated in a monopolistic environment, although often still under government influence. Interconnection between operators and the licensing of new entrants into the market have brought new regulatory responsibilities.

There is general agreement on the reasons for regulation. It promotes universal service through licensing conditions and efficient interconnection. It fosters competition to supply good quality, diversified products at acceptable prices. It limits anti-competitive behaviour and fosters a favourable investment climate. It optimises scarce resources such as the radio spectrum and the numbering system. And it can be a powerful tool for the protection of consumer rights.

Regulators have numerous responsibilities and use various tools, including:

- **Licensing –** granting of rights to telecommunication networks and services and establishing their responsibilities to contribute to national policy objectives, for example universal service
- **Management and licensing of the radio spectrum –** in a way that maximises the value of this limited national resource
- **Competition policy –** creating an environment conducive to competitive entry and **managing mergers** and acquisitions in the telecommunications sector to head off anti-competitive practices
- **Interconnection –** to ensure that new entrants are not handicapped by restrictive interconnection policies of incumbent operators, such as inflated interconnection charges
- **Numbering –** developing a national numbering plan, allocating numbers, and managing numbering resources, are as important to voice and data communications as physical addresses are to the postal system, and are key to ensuring easy access to networks and services
- **Equipment type approval –** developing and monitoring technical standards for equipment that connects to the networks
- **Universal service/universal access –** extending networks and connections to households and communities, which are handicapped by distance or poverty
- **Telecommunications Development Funds (TDF)** – establish and manage TDF to support investment in rural and under-served areas and to promote community access solutions in those areas
- **Price regulation –** particularly for non-competitive services provided by dominant providers, such as basic local telephony
- **Quality of service –** today's tendency is to focus on the quality of basic telephone service (response to repairs, amount of time on waiting lists, directory enquiries, etc) rather than on value-added services
- **Consumer protection –** defining consumer rights, drafting appropriate legislation, education and communication programmes

Regulating the fast changing ICT environment to meet modern objectives presents different challenges to those found in the old monopolistic telecommunications environment. The main issues to be addresses by today's generation of policy makers and regulators, such as universal service, tariffs, and prices, are outlined in the following section.

Another vision of regulation, by Lawrence Lessig

We have the opportunity to preserve the original principles of the Internet's architecture and the chance to preserve the innovation that those principles made possible. But that opportunity will require a commitment by us, and by government, to defend what has worked and to keep the Net open to change – a regulation to preserve innovation.

The choice is not between regulation and no regulation. The choice is whether we architect the network to give power to network owners to regulate innovation, or whether we architect it to remove that power to regulate. Rules that entrench the right to innovate have done well for us so far. They should not be repealed because of confusion about "regulation."

Source: http://www.prospect.org/print/V11/10/lessig-l.html

1 P Farajian, *Key Lessons in Telecommunications Reform*, Economic Commission for West Asia, 4 Feb 2003 (West Asia Preparatory Conference for the World Summit on the Information Society)

16. Policy and regulatory issues

Monopolies, competition and universal service

While most of the developed countries had achieved something close to universal service within monopolistic systems, the same was not true of developing countries. Users in urban areas experienced long delays in accessing telephones, and networks penetrated hardly at all into the rural hinterland. This gap in universal service led to debate in developing countries on the pros and cons of monopoly ownership, which was often resolved by granting exclusive rights to the incumbent operator for a specified period of time. This period before the introduction of competition was designed in part to provide a window of opportunity to make progress on universal service, and in part, to increase the capacity of the incumbent to deal with competition.

Universal service (lines per household or number of lines per 100 inhabitants) can be achieved through monopoly (as in most OECD countries) or through competition (as is recommended for most countries reforming their telecommunications sectors today). The commitment of the government to universal service as a policy goal and the capacity of the regulator to implement it are more important than the market regime itself.[1] This is particularly important in the developing world, where, despite universal service objectives (expansion of the network and increased number of subscriber lines), the trend is to focus on universal access to ICT. Universal access focuses on 'community access' to telecommunications facilities, particularly where it is not economically feasible to provide lines per household.

Removing telecom tariff barriers

The creation of the World Trade Organisation in 1995 gave impetus and renewed force to the negotiations that were underway on trade in telecommunications. In 1997 they resulted in agreement on a protocol and related documents setting out principles for competition, interconnection, universal service, licensing processes and the independence of the regulator. Countries that signed on to the Agreement on Basic Telecommunications set out on a course that will lead to the removal of trade barriers in the telecom sector and require adherence to agreed regulatory principles that keep the incumbent operator from taking advantage of its close relationship with government, which is often still a major shareholder.

The WTO agreements opened the way for cash-rich telecommunications operators to enter developing country markets in the second half of the 1990s. Those same developing countries are struggling to entice foreign investment in the weaker economic climate that began in 2000.

The sequencing of regulation, privatisation and competition

The introduction of privatisation, without at the same time establishing regulation and opening markets to competition, can increase the power of the monopoly provider and delay network expansion. [2]

The early establishment of independent regulation increases investor confidence; regulation can prevent the incumbent operator from creating barriers to the entry of new competitors, for example by limiting the transfer of numbers when people switch from one service provider to another, or by delaying interconnection arrangements. The creation of a regulatory authority before privatising increases telecom investment and stimulates progress towards universal service.

Maintenance of a monopoly following privatisation – an option many developing countries have chosen to allow the operator a period of exclusivity to gear up for competition and make progress on universal service – can in fact delay network expansion. Privatisation is most effective when paired with the introduction of competition.

Monopoly and growth of connectivity

Countries that privatized by granting monopoly advantages have seen connections grow at 1.5 times the rate under state monopolies but only half as fast as the rate in Chile where the government could issue competing licenses.

Source: Farajian, *Key Lessons in Telecommunications Reform*, p. 5

1 S O'Siochru, *Universal Service, Policy and Regulation – A Review of Experience Internationally*, IDRC, 1996

2 Farajian, p. 2

Regulatory flexibility

The fact that cell phones – often with text messaging capability – have overtaken fixed telephone lines in many countries is evidence of the speed and unpredictability of developments in telecommunications. Even countries which limit rights to connect users to the network to one or more national operators for a period of exclusivity following privatisation, need to allow for experimental applications at the local level to deliver the first mile of connectivity and speed progress towards universal service. Innovation can be organisational as well as technical. Co-operative local ownership models, and the use of satellite and WiFi[3] technologies are examples.

UN Secretary-General, Kofi Annan's challenge to the Silicon Valley Community on the 5th of November 2002

"We need to think of ways to bring wireless fidelity (Wi-Fi) applications to the developing world, so as to make use of unlicensed radio spectrum to deliver cheap and fast Internet access."

Source: http://www.w2i.org/pages/wificonf0603/manifesto.html

Industry self regulation

Self regulation by industry groups is an alternative to regulation.[4] Industry establishes a code of standards or guidelines and encourages voluntary adherence to its implementation. Compliance with the code is expected to increase consumer confidence in the product or service on offer. To be effective self regulation needs to be monitored by industry and the codes should be widely known to the public.

Self regulation often develops as a response to threats of regulation or legislation – it is more prevalent in North America than in Europe. The problem with it is that control of the regulation is transferred from the government to private enterprise, but there is no guarantee that this will protect users' rights any more than before.

Self-regulation in Malaysia

The Malaysian Communications and Multimedia Commission (http://www.mcmc.gov.my/mcmc/) is the regulator for the converging communications and multimedia industry. The MCMC is also charged with overseeing the new economic, technical, consumer protection and social regulatory framework for the converging industries of telecommunications, broadcasting and on-line activities. The MCMC set up the Communications and Multimedia Content Forum (http://www.cmcf.org.my/), with representation from various different industry and consumer bodies to govern content and address content related issues disseminated by way of electronic networked medium. A self-regulatory body, CMCF will govern content by self-regulation in line with a Content Code, drawn up after a long process of consultation.

But this consultation and proposed self-regulation did not stop the police raid on independent news website Malaysiakini in January, 2003 because of a letter published on the site. The police confiscated 15 computers and four servers, and although they have returned most of the equipment, two computers are still being held for possible use in court as evidence.

Source: http://www.hrw.org/wr2k2/asia8.html, http://www.malaysiakini.com/news/2003012000018962.php, http://www.seapabkk.org/

Privacy rights of internet users

In an effort to stave off Congressional action, the US web community has devised a self regulatory regime including guidelines calling for website operators to devise privacy protection policies and post them on their websites.

Source: *Trends in Telecommunications Reform 2002*, pp. 27-28

Deregulation

Deregulation in the telecom sector allows a whole new host of businesses to provide entertainment and communication options direct to home and business. Rights of way and the wires that connect long-distance carriers to homes and businesses have emerged as expensive

3 Short for wireless fidelity – the popular term for high frequency wireless local area networks.

4 International Telecommunications Union, *Trends in Telecommunications Reform 2002*, pp. 27-28

real estate. As long-distance telephone services face increasing competition, access to consumers through these rights of way have become new profit centres. This threatens community control over local resources and demonstrates the unexpected risks that may be inherent in the tide towards deregulation.

Regulatory independence

The ITU defines a separate regulator as one that is independent – in terms of finance, structure and decision-making – from the operator and the relevant government ministry.[5]

The extent to which the regulator is perceived to be independent of political control – and separate from other telecommunication bodies – is a key factor in the confidence that industry and the public have in its decision-making and its capacity to attract foreign investment. Statutory provisions governing the appointment and removal of officials, reporting requirements and financial autonomy provide some guarantee of independence. But the regulator needs to be vigilant to achieve functional independence, particularly if the government maintains a significant stake in the telecommunications operator.

Bringing internet costs down – national and regional internet exchange points

Internet traffic between users, particularly in the same country or region in Africa, is often directed to international exchange points (backbone providers) largely in G8 countries.[6] The local ISPs pay the cost of the physical link and of purchasing bandwidth once they get there. This results in a reverse subsidy to the developed country providers from the local ISPs, and has the effect of encouraging the location of Southern websites in the North. This is the case, for example, of the United Nations office in Kenya.

The creation of national and regional Internet Exchange Points is one way of addressing this problem but it requires an organised ISP sector and an environment of trust and collaboration which can be fostered by the regulator – and by regional collaboration on regulatory issues.

Regional regulation

The trend towards regulation places a heavy burden on the limited ICT skills base in many developing countries and puts the staffing and training of regulatory institutions in developing countries high on the development agenda. A regional approach may help mitigate this problem. A number of regional associations of telecommunications regulators have been created (for example the Telecommunications Regulatory Association of Southern Africa – TRASA). Caribbean countries have gone one step further and established a regional regulatory authority.

---

5 *ibid*, p. 28

6 African Internet Service Providers Association, *The Halfway Proposition: Background Paper on Reverse Subsidy of G8 countries by African ISPs*, October 2002, http://afrispa.org

17. Decision-making processes

All players agree in principle that good decisions derive from broad-based inputs, transparent processes for reconciling different interests and publicly accessible policies, laws and regulations. The two examples here illustrate the fact that it becomes more difficult to maintain open and transparent decision-making as the political stakes increase. In practice it is difficult to achieve ideal conditions with respect to national ICT policy, the management of the internet and the international telecommunications reform agenda – the three decision arenas that have been discussed in this chapter.

The United Nations system – broad umbrella of the ITU, the World Bank and the WTO – is largely a system of governments. National delegations to discussions within these bodies are more open to including different stakeholders than in the past. And the UN has granted observer status to many non-governmental organisations. Nevertheless, when power is at stake, decision-making is held close to the chests of governmental elites.

The internet itself can be a powerful tool to increase access to information and knowledge, and thereby increase transparency of decision-making and create the conditions for accountability. But it is not easily accessible everywhere and many people lack the skills to use it to further their own objectives. Many more lack the knowledge required to engage in debate on the complex commercial, technical and political issues that frame its management.

This chapter has referred to – but not addressed in detail – the role of big corporations in decision-making on ICTs. Recent corporate history has shown how easy it was to misrepresent corporate operations and assets; it underlines the importance of regulations that separate board and executive and accountancy and advisory functions. The quality of future decision-making in both global and national ICT sectors will depend very much on the quality of corporate governance.

Expanding pay phones in Sri Lanka

The Telecommunications Regulatory Commission of Sri Lanka identified problems with the supply of pay phones – low penetration, concentration in urban areas and high costs for customers. It advised the government to adopt pay phone subsidies with a goal of installing 100 new pay phones in each district and recommended limits on the amount of the subsidy and on the number that could be assigned to any single operator. It further recommended a time limit on the subsidy program.

The government accepted the recommendation and directed TRCA to implement it using its own resources.

Source: *Trends in Telecommunications Reform 2002*, p. 25

Selecting a second national operator in South Africa

The ending of South Africa Telkom's period of exclusivity through the licensing of a second national operator (SNO), was foreseen in the first post-apartheid Telecommunications Act passed in 1996. In spite of the existence of an independent regulator – the Independent Communications Authority of South Africa – the process has been widely questioned; the first round of bidding failed to produce a result that was accepted by the government. Authority rejected two bids for the 51% foreign equity stake in the SNO. The second round is now approaching completion.

Source: http://archive.mg.co.za/nxt/gateway.dll/PrintEdition/MGP2003/3lv00103/4lv00248/5lv00288.htm

Influencing national policy

To enable broad-based participation in national policy requires a high level of public awareness of the issues, which is reflected in the attention they receive in local media. Media messages need to be in a language and style accessible to the public. The internet is a powerful tool but it does not reach all users. It must be used for communication and information exchange where possible, but its limitations as a tool for broad dissemination must be recognised. The public needs to be empowered through strong civil society organisations to articulate its views; the CSOs themselves need to master lobbying techniques and learn how to connect with government, for example by creating coalitions of civil society organisations concerned with ICT issues, or by strengthening civil society voices within existing computer and communications forums.

On the regulatory side the key is clear policy and legislation that creates an independent regulator that operates at arms length from government and other interests, and

is seen to be so doing. The policy, legislation and regulatory decisions must be in the public domain. Public consultations should be organised on all issues that have public impact. Here again, the extent to which civil society and the private sector are themselves vibrant and organised will impact on their capacity to collaborate effectively in regulatory processes.

All of these conditions ultimately depend on democratic, transparent and accountable government free from the pressure of special interests and corruption.

Influencing internet management

Opening up internet management is a challenge because of the lack of recognition given to the importance of the internet by many governments, the technical nature of the issues at stake, and the other pressures on relatively small communities of experts. This is particularly the case in developing countries but it is also true everywhere outside the ICT mainstream.

Joining up for a free membership in ISOC and becoming a member of a national chapter, or establishing one, would seem to offer one of the best opportunities for strengthening the local internet community and building a platform from which to influence internet decisions. This may be a long-term solution, when the fast paced internet world calls for short term interventions. Current debates on ICANN suggest a real fear that decisions that set the future course for the internet will be made without the participation of the growing number of users in developing countries.[1]

Ideas have been suggested to make ICANN responsive to a broader community of users. These include producing ICANN documents in languages other than English, exploiting local channels – websites, print media, radio – for the dissemination of news and information, creating ambassadors to represent and promote ICANN in countries where it is little known, sponsoring developing country participation in ICANN meetings, and opening up regional seats for election on the ICANN Board. Ironically, after ICANN opened up its Board to members elected online by internet users on a regional basis, and thus exposing itself to criticism from within, it then stepped back and refused to continue with this unique (in internet governance) experiment in democracy.[2]

The newly elected President of ICANN has indicated interest in stimulating developing country government, business and consumer participation in ICANN's work. A step in this direction is the establishment of an 'at large' advisory committee (ALAC), to provide advice in relation to the community of individual internet users. ALAC members have been appointed on an interim basis by the ICANN Board. ALAC is helping to organise local and regional groups to engage internet users and disseminate news of its programmes and decisions. Once regional structures are in place they will elect new ALAC members. Since these groups are intended to be self-organising and self-supporting, they will not be easy to establish in developing countries. And they are advisory rather than decision-making bodies. They do however offer a way into ICANN's processes – they are expected to promote structured involvement and informed participation of the global internet community in ICANN.[3]

Influencing the international agenda

Developing countries are hampered in their relations with intergovernmental decision-making bodies, including the ITU, WB and WTO, by the fact that expertise in any given area is normally stretched extremely thinly. This is particularly the case with ICT expertise, which is a new area, not always recognised in developing countries as being an essential ingredient of development.

Civil society is also hampered - in its case, by the fact that it does not participate as a full partner in the deliberations of most United Nations family organisations. The UN is, for the most part, a system in which decisions are taken by governments. The one notable exception is the International Labour Organization in which Ministries of Labour, trade unions and employers organisations all have seats on the Governing Body. We have seen also that telecommunications business has always played a role in ITU although not as members of its Governing Council.

Louder Voices, a 2002 study by the Panos Institute and the Commonwealth Telecommunications Organisation4[4] , calls for a series of measures to overcome the obstacles to effective developing country participation in international ICT decision-making. The report recommends that the international community promote awareness of the role of ICT in development, provide accessible and independent research, analysis and information, and make meetings more accessible to developing countries. It recommends to developing country governments that they improve information flows, coordination and knowledge

1 A Kapur, *Why ICANN Needs Fresh Blood: A Deeper View*, March 26, 2003, http://www.circleid.com/artcles/2580.asp

2 For a former Board member's view, see http://cyber.law.harvard.edu/is99/governance/auerbach.html and http://www.eff.org/Infra/DNS_control/ICANN_IANA_IAHC/Auerbach_v_ICANN/

3 http://alac.icann.org/announceents/press-release-26jun03.htm

4 Commonwealth Telecommunications Organisation and Panos Institute, *Louder Voices: Strengthening Developing Country Participation in International ICT Decision-making*, July 2002.

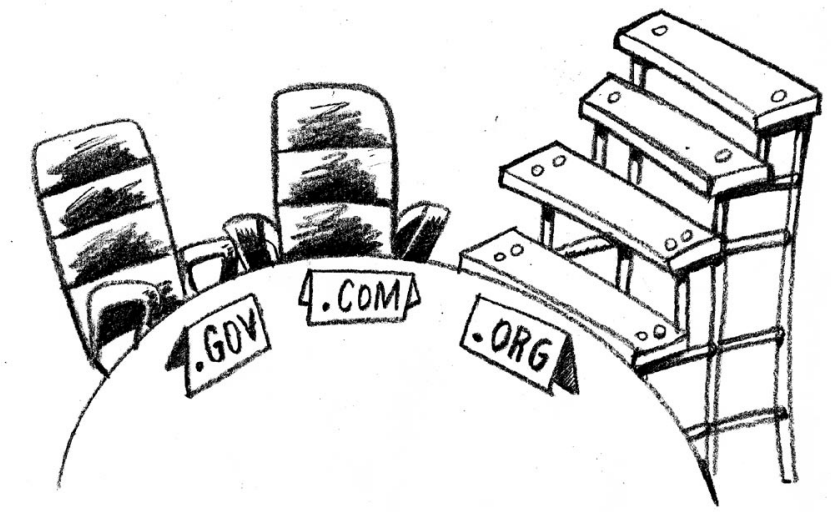
management within the sector, engage all stakeholders in policy processes, make better use of resources available for participation and build regional alliances for maximum impact in decision processes. It also proposes a series of programmes to build regional centres of specialised ICT knowledge, establish web resources and fund small-scale research.

All of these measures should be designed to strengthen non-governmental ICT organisations in developing countries as well as governments.

They are in a sense demand-side steps that will, if successful, eventually strengthen developing country voices in international organisations where ICT decisions are made.

There is room also for supply-side changes that see the big players themselves listening more carefully not only to developing countries but also to global civil society.

The following case shows both the problems and the potential of engaging in the international process leading to the World Summit on the Information Society.



World Summit on the Information Society – Geneva 2003, Tunis 2005

The convening by ITU and its partners of the WSIS is a major achievement for all those who believe that information has long been the missing element in the development equation.

It is the first Summit to take place in two sessions – the first in Geneva in 2003, the second in Tunis in 2005. The Summit was carefully prepared by a series of regional meetings – with all sectors represented. And global preparatory commissions which are led by governments. The problem with Summits of this kind is that governments must agree to the principles and action plans that emerge from them well in advance of the meetings themselves.

ITU set up a bureau specifically to facilitate civil society participation. Civil society achieved a victory in the February, 2003, Prepcom2 by getting some content included in the official drafts to be considered again in September. But then in the later Intersessional meeting, many of the issues regarded by civil society as key were omitted from the working documents for the Declaration of Principles and the Action Plan, despite the stress put on them by the civil society submissions. The discontent increased in the September, 2003, Prepcom3 meeting, where the civil society press release stated that if the final Declaration of Principles and the Action Plan did not reflect social priorities instead of market-based ones, civil society would not lend credibility to the Summit nor its results.

For the Summit itself, the Communications Rights in the Information Society (CRIS) campaign organised a day of debate within WSIS in Geneva to ensure that civil society voices are heard, and other groups, mostly from outside the process, decided to organise an alternative event, parallel to the Summit. The many civil society groups believe that the Summit documents do not reflect the fundamental inequalities that govern the global information society, and prepared their own declaration of principles, at variance with the official documents. The processes was not perfect but civil society made itself a force to be reckoned with in this most global ICT game in town.

Sources: http://www.itu.int/wsis, http://www.worldsummit2003.de/, http://prepcom.net/wsis, http://www.wsis-cs.org/index.html, http://www.geneva2003.org/wsis/indexa01.htm, http://www.wsis-cs.org/africa/.

Specific issues in internet policy and regulation / part 4

18. Gender and ICTs

"Women constitute 50 per cent of the population but do 60 per cent of work, earn one-tenth of the income and own 1/100 of the assets".[1]

The digital divide in access to ICTs, between the developed and developing world, is the result of various factors including poverty, lack of resources, illiteracy and low levels of education. In many societies women are the most impoverished with the least access to resources and with little control over decisions that affect their lives. For this reason, women are on the wrong side of the digital divide, with limited access to and control over ICTs.

When considering the factors that contribute to these inequalities it is important to understand the ways in which ICTs are allocated between women and men (the gendered allocation of ICTs), the different opportunities that exist for men and women with respect to education, training and skills development, employment and working conditions, content development and access to power structures and decision-making processes.

Beyond questions of access to technology and software, training programmes for women should focus on how to find, manage, produce and disseminate information, and how to develop policies and strategies to intervene effectively in and make use of new media. Other major concerns are illiteracy and language as obstacles to information access; the need to break down gender and cultural barriers to women's access to careers in technology; and the design of software, that often does not respond to the needs of women and girls.

The table reflects the general fact that women do not use the internet as much as men. Despite the fact that there is very little reliable, sex disaggregated data, the numbers suggest that the gender digital divide is related to income and access. In low-income countries women are excluded to a greater extent, but when access improves and becomes widespread, women use the internet as much as men do. When exclusion is widespread, women suffer from it more than men do. We need to understand why this is the case.

Recommendations of the APC Women's Networking Support Programme to the Global Knowledge Partnership

- Equity principle: women and girls must be explicitly included amongst the beneficiaries of the ICT revolution
- Gender perspective in all ICT initiatives
- Promote gender-aware training and content development
- Safe and secure online spaces for women and girls
- Content for women
- Promote the global knowledge commons as part of a poverty reduction strategy
- Women in ICT decision-making
- Science and technology education for women
- Women as ICT entrepreneurs

Source: APC Women's Networking Support Programme

1 http://www.uneca.org/aisi/aisi.htm#gender

Access to and use of the internet / Women internet users, 1998-2000

Year	% total population 2001	All internet users 1998/99	2000	Year	% total population 2001	All internet users 1998/99	2000
AFRICA				Turkey	3.8		29.0
Ethiopia	< 0.1	16.0		EUROPE			
Morocco	1.3	25.0		Austria	31.9		43.0
Senegal	1.0	14.0		Belgium	28.0	38.0	40.0
South Africa	7.0	19.0	49.0	Czech Republic	13.6	12.0	43.0
AMERICA, NORTH				Denmark	44.7		44.0
Canada	43.5	38.0	47.0	Finland	43.0		46.0
Mexico	3.5	46.0		France	26.4	42.0	38.0
USA	49.9	49.0	51.0	Germany	36.4	35.0	37.0
AMERICA, SOUTH				Hungary	14.8		46.0
Argentina	8.0		43.0	Iceland	67.9		49.0
Brazil	4.6	25.0	42.0	Ireland	23.3	31.0	45.0
Chile	20.0		47.0	Italy	27.6	30.0	40.0
Venezuela	5.3		31.0	Luxembourg	22.7		38.0
ASIA				Netherlands	32.9	13.0	41.0
China	2.6	18.0	41.0	Norway	59.6		42.0
Hong Kong SAR	45.9		43.0	Poland	9.8		37.0
India	0.7		27.0	Portugal	34.9		41.0
Indonesia	1.9		35.0	Russian Fed.	2.9	15.0	39.0
Israel	23.0		43.0	Spain	18.2	19.0	41.0
Japan	45.5	36.0	41.0	Sweden	51.6	46.0	45.0
Korea (Rep.)	51.1		45.0	Switzerland	40.4		36.0
Malaysia	23.9		42.0	United Kingdom	39.9	38.0	46.0
Philippines	2.5	43.0	49.0	OCEANIA			
Singapore	36.3		47.0	Australia	37.2	43.0	47.0
Taiwan	33.6		44.0	New Zealand	28.1	24.0	47.0
Thailand	5.6		49.0				

Source: Compiled from ITU, *World Telecommunication Development Report*, 2002; United Nations, *The World's Women 2000: Trends and Statistics*; UNDP, *Human Development Report*, 2001.

All people and groups have the right to access and effectively to use the information and knowledge required in order to address their developmental needs and concerns. This is the strategic starting point for all those concerned with gender equality and social transformation.

Education, training and skills development

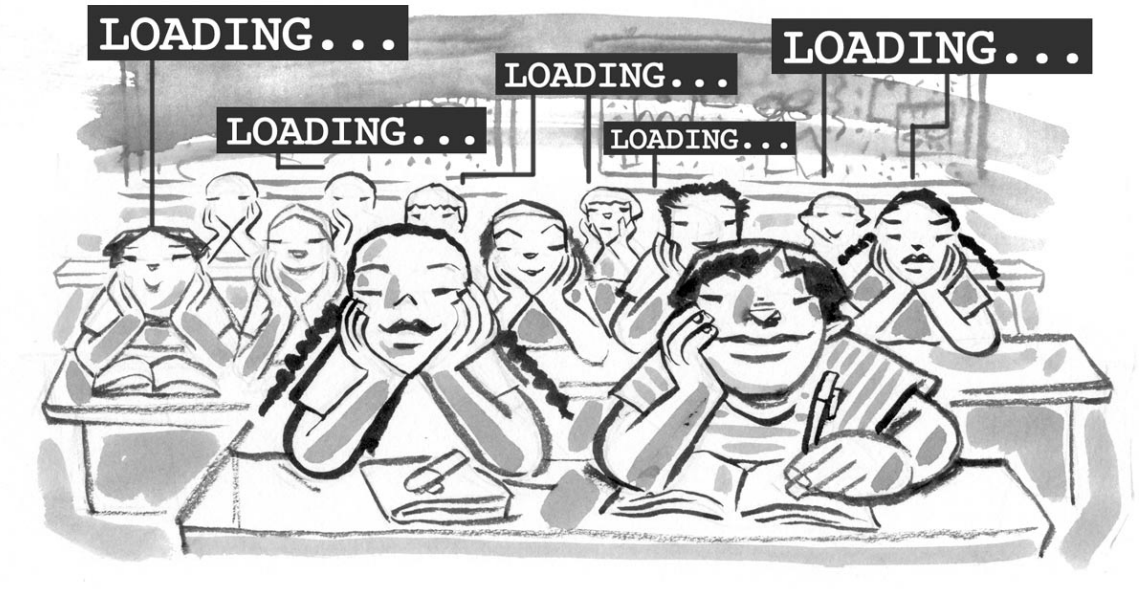
Education, training and skill development are critical to ICT interventions. Problems with ICT training for women in the past included the fact that they were often ad-hoc, alienating and not customised to women's needs. Solutions point to learning practices that should be extended to girls and women, made gender-sensitive (making training women-specific, ensuring ongoing user support, and mentoring in the communities where women live), and deepened (for women as users, technicians, policy and change-makers).

Industry and labour

In the ICT industry, labour is highly sex-segregated. Women are found in high numbers in the lowest paid and least secure jobs. The gender dimension of ICTs also affects telework, flexi-time, and work from home arrangements, where women have few rights, meagre pay, and no health, social or job security. A woman's wage-labour outside (or inside) the home as a result of the new technologies does not necessarily entail a change in the family division of labour. Men still get out of doing the housework, and women find themselves with dual or triple burdens. Poor working conditions, long hours and monotonous work routines associated with ICTs are often injurious to women's health.

In its employment report released in January 2001, the ILO reveals a "digital gender gap", with women underrepresented in new technology employment in both developed and developing countries. The ILO report also finds that patterns of gender segregation are being reproduced in the information economy.

According to Professor Swasti Mitter of the United Nations University Institute for New Technologies (UNU/INTECH), who directed a UNIFEM sponsored research project on gender and new technologies, the growth of transnational teleworking has opened up many opportunities for women in the South, including data entry, medical transcription, geographical information systems and software production: "The work of UNU/INTECH in the context of China and Vietnam shows that globalisation has brought new opportunities to young women with familiarity with English in new, service sector jobs, but has made a vast number of over 35-year-olds redundant, either because they are in declining industries, or have outdated skills."



Content and language

What content will predominate on the internet and in new media? Who creates it? What is its cultural bias? Are women's viewpoints, knowledge and interests adequately reflected? How are women portrayed? These are some of the questions that have been raised relating to content, whether in internet spaces, video games or virtual reality.

Women's viewpoints, knowledge and interests are not adequately represented while gender stereotypes predominate on the internet today. Some of these concerns are an extension of those formulated in relation to sexism and portrayal of women in the media in general. But they also relate to a broader range of issues such as the need for women to systematise and develop their own knowledge and perspectives and make sure they are adequately reflected in these spaces.

The dominance of English language content, often from countries in the North, on the internet, is another major concern raised by women's organisations. Language barriers to information access require the development of applications such as multilingual tools and databases, interfaces for non-Latin alphabets, graphic interfaces for illiterate women and automatic translation software.

Power and decision-making

Although women are acceding in ever-greater numbers to jobs and expertise with ICTs, the same is not necessarily true of their access to decision-making processes and control of resources. Whether at the global or national levels, women are under-represented in all ICT decision-making structures, including policy and regulatory institutions, ministries responsible for ICTs, boards and senior management of private ICT companies. One problem is that decision making in ICTs is generally treated as a purely technical area (typically for men experts), where civil society viewpoints are given little or no space, rather than a political domain. Deregulation and privatisation of the telecommunications industry is also making decision making in this sector less and less accountable to citizens and local communities, further compounding the problems experienced by women in gaining access to decision making and control of resources.

The 'Empowerment Framework': welfare, access, conscientisation, mobilisation, control

Welfare is defined here as the lowest level at which a development intervention may hope to close a gender gap. We are here talking about women being given these benefits, rather than producing or acquiring such benefits for themselves.

Access – the first level of empowerment – is the opportunity to make use of ICTs – both in terms of technology and information and knowledge. Control refers to the power to decide how ICTs are used, and who has access to them. Women's access to ICTs and control of them (or lack thereof) is dependent on many factors. Factors such as gender discrimination in jobs and education, social class, illiteracy and geographic location (North or South, urban or rural), influence the fact that the great majority of the world's women have no access to ICTs or to any other sort of modern communication system, and possibly will not in their lifetime. It is logical to deduce that as information dynamics accelerate their migration towards the Internet, people without access are bound to suffer greater exclusion. But there are also voices that insist that connectivity in itself is not enough, and that providing women with computers and modems is not sufficient for them to resolve their development problems.

Conscientisation is defined as the process by which women realise that their lack of status and welfare, relative to men, is not due to their own lack of ability, organisation or effort.

Mobilisation is the action level which complements conscientisation. Firstly it involves women's coming together for the recognition and analysis of problems, the identification of strategies to overcome discriminatory practices, and collective action to remove these practices.

Control is the level that is reached when women have taken action so that there is gender equality in decision making over access to resources, so that women achieve direct control over their access to resources.

Therefore these five levels are not really a linear progression, as written above, but rather circular: the achievement of women's increased control, leads into better access to resources, and therefore improved socio-economic status.

In evaluating a project, we need to ask ourselves whether the project is intervening merely at the level of providing improved welfare, and access to information. Or is it enabling women's participation in a process for increased conscientisation and mobilisation, as a means for increased action and control?

Source: S Longwe, *The Process of Women's Empowerment*, http://www.sarpn.org.za/documents/d0000055/page6.php

Pornography, trafficking, violence against women, and censorship

The picture that emerges from most analyses of new information and communication content is of masculinist rhetoric and a set of representations that are frequently made sexual and often sexist. Pornography, email harassment, 'flaming' (abusive or obscene language), and cyberstalking are well documented. It is estimated that 10 percent of sales via the Internet are of a sexual nature, whether in the form of books, video-clips, photographs, on-line interviews, or other items. New technical innovations facilitate the sexual exploitation of women and children because they enable people easily to buy, sell and exchange millions of images and videos of sexual exploitation of women and children.[2] These technologies enable sexual predators to harm or exploit women and children efficiently and, anonymously. As a result of the huge market on the Web for pornography and the competition for audiences among sites, the pornographic images have become rougher, more violent, and increasingly degrading. The affordability of and access to global communications technologies allow more users to carry out these activities in the privacy of their home.[3]

Even more disturbing is the use of the internet as a tool in the prostitution and trafficking of women. In 1995 an estimated 1.8 million women and girls were victims of illegal trafficking, and the numbers are growing. The internet is used in multiple ways to promote and engage in the sexual exploitation and trafficking of women. Pimps use the internet to advertise prostitution tours to men from industrialised countries. The men then travel to poorer countries to meet and buy girls and women in prostitution. Traffickers recruiting women from the Baltic States use the Web to post advertisements for unlikely jobs in Western Europe (such as waitress or nanny). Information on where and how to find girls and women in prostitution in cities all over the world is posted on commercial Web sites and non-commercial newsgroups.[4] In response to the growing problem, the Council of Europe in 2001 established a working group to study the impact of new information technologies on trafficking in human beings for the purpose of sexual exploitation

There are numerous organisations working on the issues of women's trafficking which have done much to impede the use of the internet for trafficking in women and children, and the explosion of pornography on the internet While recognising that traffickers and pornographers have moved their businesses to the internet, women's organisations have also been aware of the dilemma of calling for government measures to curb this.

One of the fiercest debates in the area of internet rights regards the issue of freedom of expression and censorship. Some organisations have used the presence of pornography on the internet to call for stricter policies for monitoring and censuring content on the internet, including the development of software devices that would track down the creators and consumers of pornographic materials. But child porn on the internet is as illegal as it is offline/outside. There is no need to create special laws for cyberspace. Some women's organisations have been at the forefront of pointing out the danger of inviting censorship measures that could very easily be extended to other content areas, and limit freedom of expression far beyond the issue of pornography and trafficking.

Legislation can be interpreted widely, leaving it open for states to decide what they would consider "illegal" or "harmful practices."

The priority is that women should be informed, aware and included in the discussions and debates taking place around this trend, and consulted in the development of any policies and practices that are advocated by state agencies and other bodies involved.

In this spirit, UNESCO is already carrying out a number of research and awareness-raising projects to combat trafficking in women and children in the Asia-Pacific region, and has been collaborating with the Open Society Institute in the creation of the 'Stop Trafficking' network in Central and Eastern Europe, as well as in Central Asia. In December 2002, UNESCO also co-hosted an international symposium on the theme of freedom of expression in the information society, where discussion focused on three issues: the new possibilities and limitations offered by cyberspace with regard to freedom of expression; all the obstacles limiting freedom of expression in cyberspace; and the issue of regulation of content in cyberspace. The participants concluded that:
"We must resist the temptation to demonise the Internet. The offences committed on the Internet are not particularly original (apart from attacks by hackers); they reflect

2 Rich, F (2001)

3 Hughes, D M (2002)

4 Hughes, D M (2001)

behaviours that are specific to social life, and which already found carriers in the traditional media. Thus we need to look at the Internet as a tool for democracy, and not from the angle of its real or potential failings."[5]

Current initiatives to regulate and control the internet, both in relation to content and use, strike at the heart of the power of new technologies – a system of tools that allows people to communicate with one another, one-to-one, one-to-many, many-to-many, across traditional and entrenched power structures. To threaten this potential, through initiatives which censor, monitor and survey people, movements, actions, information and communication, will severely limit peoples abilities to learn, network and participate in the decision-making processes which govern their lives.

Violence against women on the internet

In this series, we will explore the various ways in which violence against women is facilitated through the use of the Internet, as well as ways in which the Internet may be used as a site of resistance to such violence. Violence against women is a critical social problem that affects all of us in some way. Whether we have directly experienced abuse, know a friend who has been victimized, or have been confronted with the myriad other forms such violence take, it impacts how we view the world and shapes our experiences and opportunities.

Source: http://cyber.law.harvard.edu/vaw02/

Module 5: The Internet as an Organising Tool

In the past three Modules, we have looked at serious social problems involving violence against women and the role of the Internet in perpetuating it. In this Module, we will turn the tables and explore the power of the Internet as an organizing tool to fight violence against women.

The Internet has become a critically important form of media. News dissemination through the Internet is unprecedented. Never before has news been distributed so widely and instantaneously as it is currently on the web.

All of us have had experience with Internet activism in some way. Friends send emails asking us to sign petitions; news services inform us of something important happening in the field; or a political organization tells us about some impending crisis, like an environmental group updating its listserve on the possibility of drilling for oil in Alaskan nature reserves.

Source: http://cyber.law.harvard.edu/vaw02/module5.html

Source: Berkman Center for Internet & Society BOLD site for "Violence Against Women on the Internet'

The Centre for Mayan Women Communicators (CMCM)

The CMCM in Guatemala is a non-profit organisation whose web site is hosted by the Sustainable Development Networking Programme, which also provides technical support: www.sdnp.undp.org. The Centre's activities are determined by indigenous women who participate and co-ordinate through a directive committee. The functions of the Centre are primarily to unite and communicate, develop skills in communications technology to enable them to 'ameliorate' the way they are perceived, viewed in the world and in the local media. Video and photography are often the tools used for research reflection and organisation. Using the (internet) services offered by the Centre, Mayan women living in isolated communities have the opportunity to sell their products by accessing alternative markets thus keeping their traditional crafts and artwork alive.

Source: www.rds.org.gt/cmcm/coop2n.html.

5 UNESCO (2002)

Gender Evaluation Methodology (GEM)

GEM, developed by the APC's Women's Networking and Support Programme, is a guide to integrating a gender analysis into evaluations of initiatives that use Information and Communication Technologies (ICTs) for social change. It is a framework that provides a means for determining whether ICTs are really improving women's lives and gender relations as well as promoting positive change at the individual, institutional, community and broader social levels.

The guide provides users with an overview of the evaluation process (including links to general evaluation resources) and outlines suggested strategies and methodologies for incorporating a gender analysis throughout the evaluation process. GEM does not contain step-by-step instructions to conducting evaluations and it is not simply an evaluation tool. It can also be used to ensure that a gender concerns are integrated into a project planning process.

GEM is an evolving guide: the developers encourage critical thoughts and creative adaptations in its practical use.

Source: http://www.apcwomen.org

Strategies to incorporate gender considerations into ICT policy-making

The following recommendations relate to strategy and lines of action that will enable women to overcome the many obstacles that they face, and help guarantee them more equitable access to new and emerging communications technologies and electronic information sources.

- Promote the access of women, girls and women's organisations to new and emerging communications technologies and computerised information resources
- Promote the development of computerised information resources on issues related to the advancement of women
- Support the development of initiatives of women and citizens' groups in the field of computer networks that promote the advancement of women and gender equality
- Support women and girls' access to training in using computer networks and promote a gender perspective in training and methodology in the field of new technologies
- Promote equal access of women to advanced technical training and careers in computer communications
- Promote and support the equal participation of women in international and national decision-making relating to use of communications infrastructure and access to computer networks
- Create content that reflects women's needs and voices
- Facilitate and encourage the involvement of women in technological innovation

Conclusion

As pointed out in the five-year review report of the implementation of the Beijing Platform for Action, traditionally, gender differences and disparities have been ignored in policies and programmes dealing with the development and dissemination of improved technologies. As a result, women have benefited less from, and been disadvantaged more by, technological advances. Women, therefore, need to be actively involved in the definition, design and development of new technologies. Otherwise, the information revolution might bypass women or produce adverse effects on their lives. The outcome of the five-year review recommended that further actions and initiatives have to be explored and implemented to avoid new forms of exclusion and ensure that women and girls have equal access and opportunities in respect of the developments of science and technology.

APC-WNSP : Mapping gender and ICT policy advocacy

Since 1993, APC-WNSP has played a leading role in gender and ICT advocacy in national, regional and international arenas. Our ICT policy work began during the Fourth World Conference on Women in 1995. Since then, the 'gender and ICT' agenda has steadily gained legitimacy as a serious area of concern through painstaking work by women's groups and gender and ICT advocates. During the UN World Summit on the Information Society (WSIS) process, we continue to work with civil society groups to ensure that a gender perspective is integrated into all deliberations and drafting of documents of the Summit.

ICTs offer immense possibilities for reducing poverty, overcoming women's isolation, giving women a voice, improving governance and advancing gender equality. This potential will only be realised if all factors which contribute to the current 'gender digital divide' are recognised and addressed in the WSIS process and in all ICT policy-making spaces. Nonetheless, there continues to be a serious lack of acknowledgement and commitment to redressing gender imbalances in women's participation and benefits from the envisioned 'Information Society' at all levels of policy.

Our message is simple and clear: if these concerns are not addressed we face the danger that WSIS and other policy processes, will fail in addressing the needs of women, and will contribute to reinforcing and reproducing existing inequalities, discriminations and injustices.

The following guide provides an overview of key gender and ICT policy concerns.

1. Acknowledge, protect and defend Women's Rights in the Information Society

Human rights and freedoms, of which women's human rights and freedoms are an integral part, must be located at the core of the information society. In order to be realised, human rights and freedoms must be interpreted, enforced and monitored in the context of the Information Society.

All women and men, communities, nations, and the international community have the right to access and effectively use the information and knowledge they need to address their development concerns. This is the strategic starting point for all concerned with gender equality and social transformation. In a globalised world that continuously undermines localised democratic institutions, the Internet provides an essential means for defending and extending participatory democracy.

2. Gender equality, non-discrimination and women's empowerment are essential prerequisites for equitable and people-centred development in the 'Information Society'

An equitable and inclusive 'Information Society' must be based on the principles of gender equality, non-discrimination and women's empowerment as contained in the Beijing Declaration and Platform for Action and the CEDAW Convention. These are central elements of social justice, political and economic equality strategies.

Women and girls must be explicitly included as beneficiaries of the 'ICT revolution' as a fundamental principle of equality and an essential element in the shaping, direction and growth of the 'Information Society'. They must have equal opportunities to actively participate in ICT policy decision-making spaces and the agenda setting processes which shape them.

3. ICT governance and policy frameworks must enable full and equal participation

Global, regional and national ICT governance and policy frameworks can either enable full participation in the information society or inhibit people's access to the technology, information and knowledge.

Policy frameworks deal with the development of national communications infrastructure, to the provision of government, health, education, employment and other information services, to broader societal issues such as freedom of expression, privacy and security. All of these policies have implications for women and failure to take account of these will certainly lead to negative impacts for women in relation to those for men.

4. All ICT initiatives must incorporate a gender perspective

A gender perspective must be incorporated by all stakeholders involved in the process of planning, implementing, monitoring and evaluating ICT initiatives. Hence, all stakeholders must of necessity develop quantitative and qualitative indicators, benchmarks, and 'ICT for development' targets that are gender specific.

5. Every woman has the right to affordable access

Universal access and community access policies must be underpinned by an understanding of the gender and rural-

urban divide and take into account gender differences in mobility, available time, income, literacy levels, and general socio-cultural factors.

National ICT policies must create an environment where more investment is directed to the expansion of basic telephony and public ICT access infrastructure that links women and others in remote and rural areas, at affordable costs, to information resources and populations in urban areas.

6. Education and training programmes must promote gender awareness

All stakeholders must seek to empower women's and girls' access to and effective use of ICTs at the local level through gender-aware education and training programmes. Maximum use must be made of ICTs to eliminate gender disparities in literacy in primary, secondary and tertiary education, and in both formal and informal settings.

7. Women and girls have a right to equal access to educational opportunities in the fields of science and technology

Governments must design and implement national policies and programmes that promote science and technology education for women and girls, and encourage women to enter into high 'value-added' ICT careers. It is imperative to counter the reproduction of historical patterns of gender segregation in employment within the ICT sector, where men are more likely to be found in the high-paying, creative work of software development or Internet start-ups, whereas women employees predominate in low-paid, single-tasked ICT jobs such as cashiers or data-entry workers.

8. Women count: Their viewpoints, knowledge, experience and concerns must be visible

All stakeholders must support initiatives that facilitate women's and girls' ability to generate and disseminate content that reflects their own information and development needs. Women's viewpoints, knowledge, experiences and concerns are inadequately reflected on the Internet, while gender stereotypes predominate. These concerns around content relate both to issues of sexism and the portrayal of women in media generally, as well as to the need for women to systematise and develop their own perspectives and knowledge, and to ensure that they are reflected in these spaces

9. No Public Domain of Global Knowledge without women's knowledge

Human knowledge, including the knowledge of all peoples and communities, also those who are remote and excluded, is the heritage of all humankind and the reservoir from which new knowledge is created. A rich public domain is essential to inclusive information societies and must fully embrace women's knowledge including knowledge that is contextual, rooted in experience and practice and draws from local knowledge in areas of production, nutrition and health.

The privatisation of knowledge and information through copyright, patents and trademarks is ceasing to be an effective means of rewarding creative endeavour or encouraging innovation and can contribute to the growth of inequality and the exploitation of the poor. All stakeholders must promote the maintenance and growth of the common wealth of human knowledge as a means of reducing global inequality and of providing the conditions for intellectual creativity, sustainable development and respect for human rights.

10. Every woman and girl has the right to communicate freely in safe and secure online spaces

Women and girls have a right to access online spaces where they can share sensitive information, exchange experiences, build solidarity, facilitate networking, develop campaigns and lobby more effectively. They have a right to a secure online environment where they are safe from harassment, enjoy freedom of expression and privacy of communication, and are protected from electronic surveillance and monitoring.

The internet can be used to commercially and violently exploit women and children, replicate and reproduce stereotypical and violent images of women and facilitate sex-trafficking of women as well as trafficking in persons.

Policy and regulatory frameworks to address such use of the internet should be developed inclusively and transparently with all stakeholders, particularly women, and be based on the international human rights framework encompassing rights related to privacy and confidentiality, freedom of expression and opinion and other related rights.

19. Intellectual Property

19.1. What is intellectual property? [1]

Intellectual property (IP) is an intangible thing – such as an idea or innovation – that, in most parts of the world, you can own, similar to the way that you can own tangible things like a car or a plot of land. The intangible thing can be something that you have written, drawn, designed, invented, or spoken, and it can be something that you have created yourself or paid someone to create for you. Like tangible property, you can buy, sell, exchange or give away intellectual property, and you can control its use by others. However, in order for your intangible thing to qualify as intellectual property so you can gain these rights, you have to be able to distinguish it from similar things. There are many different perspectives on intellectual property and many people feel that current intellectual property regimes need to change. Some feel that these regimes need to be tightened, to apply stricter rules to the ownership and control of ideas, while others feel that there should be fundamental transformation of IP regimes to ensure equitable public access and stimulate innovation. Some even argue that IP should be eliminated in its entirety.

Inventions of the mind – ideas – are very special. All cultures and societies are built upon numerous layers of accumulated past knowledge and ideas. In the arts, medicine, education, agriculture, and industry – in almost all areas of human endeavour – knowledge and ideas lie at the base of human life and its passions.

Intellectual property rights (IPRs) emerged in the industrialised world as a means to mediate and control the circulation of knowledge, and as a means of balancing the conflicting rights of different groups involved in the generation and use of ideas of economic value. IPRs are premised on concerns that the *creators or authors* of ideas should have a material right to a fair return for their effort and a moral right not to have their ideas misrepresented.

However, ideas are not simply the product of individuals and corporations. For the most part they incorporate and build upon the traditions, collective wisdom, and understanding of social groups and societies. Sometimes they build upon natural creations and processes that have taken millions of years to evolve. Consequently, *society in general* has a social right to use ideas for the benefit of the public good – especially if they are key to social and physical well being.

IPRs attempt to balance these rights: the moral, the economic and the social.

The justification of intellectual property is that it will protect innovations and allow people to make money by sell-

1 This section draws extensively and quotes verbatim from two sources: "Why should IPR matter to civil society", by CRIS, 2003 and the IPR module of the APC/CTO ICT for civil society curriculum developed by Bridges.org.

ing their ideas. Usually the expression 'intellectual property' is used as a legal term to indicate four distinct types of protection given to intangible property:

- Patents
- Trademarks
- Copyright, and
- Trade secrets.

The rules for IP protection, such as the scope of protection and the requirements for obtaining protection, are set out and enforced in laws and regulations of national governments. While the details of national IP laws can vary, the basic principles are generally the same. In general, the IP owner is responsible for proving a violation in order to enforce IP rights.

History

Key events in the development of notions of intellectual property were the Paris Convention for the Protection of Industrial Property (1883) and the Berne Convention (1886), where the foundations of international IP law were laid. Here the concepts of international respect for copyright, automatic copyright without any need to register, and the limit of 50 years after the death of the author were introduced. The Berne Convention revision (1928) added the concept of moral rights, such as the right to have work acknowledged and not be disparaged. Again in Berne, in 1996, digital media were included in the existing rights framework. In the Trade-Related Aspects of Intellectual Property Rights (TRIPS) agreement, part of the GATT agreements of 1994, intellectual property was extended from individual works to intellectual creation, making software copyrightable. Current IP regimes emerged mainly in Europe and have increasingly been adopted in the rest of the world.

International institutions that play a role

There are a number of international treaties and agreements that aim to harmonise national IP laws across countries. Most of the key treaties are incorporated under the umbrella of the World Trade Organisation (WTO) Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), which sets out the standards for IP protection among WTO member countries. Members can use WTO mechanisms to enforce the IP protection offered by these treaties. The World Intellectual Property Organisation (WIPO) otherwise administers these treaties and drives the enforcement of intellectual property law worldwide. It also administers other international agreements on IP, including the WIPO Copyright Treaty and the WIPO Performances and Phonograph Treaty, which require signatory nations to punish people who circumvent technologies intended to protect copyrighted works. The laws that regulate patents are national laws, but the agreements such as TRIPS make sure that these laws are extended internationally.

In practice, what is established as the norm in the USA, and increasingly in the European Union, is often copied in other countries. For instance, in Korea, "the Korean Intellectual Property Office put Business Method Patents into the patent system by simply importing the US Patent Examination Guideline despite ... ifferent legal principles."[2] As with so many other things, IP developments in economically dominant countries tend to determine world trends.

Current trends in IPR

In the last few decades, three trends have emerged: corporations have emerged as the key owners of copyrighted material; the scope, depth and duration of copyright has grown hugely, to encompass not only intellectual work but also plant and life forms, and; copyright owners wield a formidable set of instruments to enforce their rights nationally and internationally.

While IPR had traditionally been used by the cultural industries to reinforce their control over 'ideas' and 'products', the threat posed by 'copying' in a digital era, has led to a renewed interest in IPR and to increased investments in the proprietorial significance of IP. In a knowledge economy, any content that is a product of the digital manipulation of data is considered intellectual property. Technically speaking, even an email message can qualify for IP protection. Some of the factors that have contributed to the consolidation of a market-based, global IP regime include the following: shrinking profits in an era characterised by technological and product convergences; economic downturn in the telecommunications and dotcoms sectors, and; the real and imagined threats to corporate profitability posed by piracy via subversive uses of technology such as MP3 and establishments such as the recently domesticated, peer-to-peer, net-based music swapping service, Napster.

IPR has affected the public's access to knowledge in the public domain and to copyrighted works, limited legitimate opportunities for cultural appropriations, stifled learning, creativity, and innovation, thus placing curbs on the democratisation of knowledge. IPR has also infiltrated into the domain of food and medicine, threatening the sustainability of indigenous knowledge and biodiversity.

Source: CRIS Campaign, "Why should intellectual property rights matter to civil society?", http://www.crisinfo.org/live/index.php?section=4&subsection=2&doc=11

2 H Nam and I Kim, "Digital Environment and Intellectual Property Rights", *Asian Internet Rights Conference 2001*, Jimbonet, 2001, p 158.

19.2. Forms of intellectual property protection

Patents

A patent is an intellectual property protection that applies to inventions or designs for inventions, which gives the inventor exclusive rights to make, use, and sell the invention for a certain period of time. Usually an invention can include a product or a process to make a product. In general, the invention must be novel, useful, and non-obvious in order to qualify for IP protection. Patents commonly cover things like devices, chemical compositions, and processes for creating devices and chemicals. Some countries offer patents for ornamental industrial designs, and new varieties of plants. As part of the application for a patent, the inventor must disclose the details of the invention or design to the public. After the period of exclusive rights has expired, anyone can use the invention or design in any way they wish. The idea behind patents is that the period for exclusive rights will encourage innovation because inventors (or those who fund inventions) will have a chance to recover their costs for research and design. Limiting this period is intended to encourage the commercialisation of the idea. At the same time, patents are intended to serve the public good by encouraging researchers to share information and limit duplication of effort. The TRIPS treaty obliges WTO member countries to protect the exclusive rights of patent holders for 20 years from the date when the application to register the patent was made. Signatory countries must adopt legislation that gives full product patent protection by 1 January 2005.

Trademarks

A trademark is an identifying feature that denotes a particular group of goods or services. It is usually some kind of distinctive sign – like a word, logo, colour combination, or musical tones – that is intended to differentiate a company's products or services from those of its competitors. It is intended that clients and consumers will associate the trademark with the goods or services of the company. Trademarks are protected as intellectual property in order to allow companies to build a reputation for their goods and services that can be associated with the identifying feature. You are not allowed to use a trademark for your goods and services that is the same as or similar to a protected trademark if it is likely to cause confusion among clients and consumers. For example, confusion is likely to be caused by a similar trademark that is used to identify similar goods and services, or to identify different products or services sold in the same market. When choosing a trademark, you have a responsibility to avoid infringement of other trademarks, and may be required to conduct a search to make sure that no one else is using the trademark. In order to protect your trademark, registration with the national authority is sometimes, but not always, required. Some countries grant protection to the first person to use the trademark in the course of business, but other countries grant rights to the first person to register the trademark. Even when not required, it is recommended that you register your trademark to ensure that you can stop others from using it. For example, if your trademark is registered, then other people will be certain to find it when they conduct a search. But once you register the trademark you have to use it within a given period of time or it could be considered abandoned. If the trademark is 'well known' it does not always have to be registered. For example, WTO member countries have to give protection to well-known trademarks (such as the McDonalds golden arches). Trademark protection is indefinite, as long as the requirements are met.

A recent source of controversy is the relation between trademarks and Internet domain names. In some countries, domain names can be registered only if the registering entity has a proven claim to that name, such as a registered trademark, or their name and the domain coinciding. In others, registration of obvious names of companies or institutions is forbidden except to that organisation. But in many countries, there is no restriction, and anyone can register a domain name that is the same as a company's or a person's name or product.

This has led to a number of cases where domain names have been challenged. These challenges have often been successful, especially when the domain has been registered with the obvious aim of selling it, sometimes after using it as a link to a pornographic or gambling site as a means of applying pressure on potential buyers. Rules

for registering domain names vary from country to country, and some are stricter than others. In the USA, for domains such as .com, now used internationally, a dispute resolution mechanism has been instituted to deal with problems of domain 'squatting'.

Another contentious issue is the use of trademarks or official logos in web pages without the consent of the owner of the trademark. Whilst the inclusion of trademarks within text is generally allowed, this is normally within the limits of fair dealing. A site that misleads the public by using trademarks or logos, will have less chance of protection from the law than one which is clearly a parody. In the latter case, issues of free speech come into play and the matter is not clear-cut. It is all very well for a trademark owner to have the right to challenge its use by a rival company (for example the producer of a Coca Cola-like beverage who makes use of the Coca Cola logo). However, when, for example, a trade union uses the logo of a company where workers are on strike to publicise the labour dispute, limiting the use of the trademark can constitute a limitation of freedom of expression.

Fox News to Franken: "Hands Off 'Fair and Balanced!'»

Fox News has filed a trademark infringement suit against humorist Al Franken for use of the phrase 'fair and balanced' in the title of his book, "Lies, and the Lying Liars who Tell Them: A Fair and Balanced Look at the Right." According to the New York Times, lawyers for Fox say the broadcaster "has trademarked 'Fair and Balanced' to describe its news coverage and that Mr. Franken's use of the phrase would 'blur and tarnish' it." The Washington Post reports that "in its fair and balanced way, Fox News refers in its suit to Franken as an 'unstable' and 'shrill' 'C-level commentator' who is 'not a well-respected voice in American politics.'"

Source: http://www.info-commons.org/blog/archives/000099.html

Copyright

Copyright is an intellectual property protection granted to literary, musical and artistic works, including drawings, poems, films, written publications, and software. It applies to original, creative works fixed in a tangible medium that is permanent or stable. It gives the creator the exclusive right to copy, publish, perform, or broadcast the work, but it does not prevent the independent creation of similar works by others. It also does not prevent the 'fair use' of the work, such as for news reporting, teaching, or research.

Copyright exists automatically once the work has been created, and does not require registration. It usually lasts for the life of the creator plus 50 years. In most cases, if the creation is made in a work setting, the employer holds the copyright for the work. Under the TRIPS treaty, corporate entities can have the copyright for 50 years from the year of publication, but under certain conditions the copyright can last much longer. For example, in the United States such a work can have a copyright for 120 years from the time of creation or 95 years from first publication, whichever is shorter. Even though copyright registration is usually not required in order to gain copyright protection, it is available in most countries; in some countries registration is considered proof of the copyright ownership. The copyright owner must include a copyright notice on the work. On a recording the copyright notice should include a symbol - ã - with the year of first publication and the name of the copyright owner. For other works the copyright notice should include a symbol or the word "Copyright", the year of first publication, and the name of the copyright owner. For example, "Copyright 2003 APC".

On the internet, copyright is more complicated. While the material is not in printed form, normally the form covered by copyright, a text on a computer screen can be printed and reproduced in hard copy. Also, internet tools such as email and the World Wide Web makes copies of material as part of the way they function. When you click on a link on a web page, your browser sends a message to the server where the document is stored, requesting a copy of a file which it converts into the visually accessible page you see on your screen. On the way to its destination, the file, perhaps containing copyrighted text, is copied and stored on several other computers. It would be reasonable to ask an author who puts his/her work on a web page whilst prohibiting its being copied: "Why do so if you know that to read the file it must be copied?" In practice, copying copyrighted material on the internet is accepted, provided it is only for the purpose of reading.

Copying music is more controversial. Modern digital technology allows easy copying of compact discs and sending of music in various formats, such as mp3, via the internet. Peer to peer (p2p) software has been developed

In the United States, the **Sonny Bono Copyright Term Extension Act** of 1998 retroactively extended the duration of copyright from the life of the author plus 50 years to the life of the author plus 70 years, in the case of individual works, and from 75 years to 95 years in the case of works of corporate authorship and works first published before 1st January 1978.

Under the Berne Convention states are required to provide copyright protection for a term of the life of the author plus 50 years. However, the convention permitted parties to provide for a longer term of protection, and between 1993 and 1996, the European Union provided protection for a term of the author's life plus 70 years. The United States, however, only provided for the minimum required by the convention. As a result, many literary works, movies and fictional characters, which were quite profitable for the copyright owners, were threatened with passing into the public domain. This included several characters owned by the Walt Disney Company; without the act, Mickey Mouse would have entered the public domain between 2000 and 2004 when early short films such as Steamboat Willie and Plane Crazy were due to reach the end of the 75-year copyright term. As a consequence of the act, no copyrighted works will enter into public domain due to term expiration in the United States until 1st January 2019, when all works created in 1923 will enter into public domain.

Source: http://www.wikipedia.org/wiki/Sonny_Bono_Copyright_Term_Extension_Act

to allow the sharing of these and other files without the intervention of a central database or a web page, that is directly between two people who are connected to the internet. The multinationals which dominate the music industry today have taken several companies, such as Napster and Kazaa, to court to try to preventhis, but the decentralised nature of modern p2p programmes makes this extremely difficult, if not impossible, to enforce, unlike the direct selling of pirated CDs in the street. Another example is the attempted prosecution of those who made available software (DeCSS), which permits DVD disks to be copied on a computer.[3]

Trade Secrets

A trade secret is confidential business information that gives its owner a competitive advantage, such as techniques, processes, recipes, or methods. Trade secrets are protected as intellectual property where they are valuable to the owner and steps are taken to keep the information confidential. They are not protected if someone else independently obtains the information. [4]

The TRIPS Armoury

A key means by which IPR has been reinforced and extended is through TRIPS and the Copyright Treaty (1996) that was negotiated by the World Intellectual Property Organisation (WIPO). These agreements have been used as a means to tie trade with IP, as templates for national legislation on IPR and for ensuring the harmonisation of global agreements such as TRIPS with local IP legislation. These global agreements have been backed by trade associations, such as the Motion Picture Association of America (MPAA), groups like the US-based International Intellectual Property Alliance (IIPA) and corporations such as AOL-Time Warner, Microsoft and IBM. These groups

"The CD will be a memory in 20 years"

"In the United States, in 10 years probably 90% of people will get 90% of their music from the Internet. In 20 years time, the record companies will distribute their products only in digital form. People will look at CDs as memories from the past. It's unquestionable."

Mark Hall (vice-president, Real One) and Rob Reid (president, Listen.com/Rhapsody) when asked about the future of digital music.

Source: *Ciberpais*, 31st July 2003, p. 6

3 See http://www.theregister.co.uk/content/4/28749.html, http://web.lemuria.org/DeCSS/, http://cyber.law.harvard.edu/openlaw/DVD/

4 Trade secrets are not normally part of ICT policy questions. However their importance can be seen in the way the SCO company has taken IBM to court for using its property in the development of GNU/Linux. See http://swpat.ffii.org/pikta/xrani/sco/index.en.html, http://www.zdnet.com.au/newstech/os/story/0,2000048630,20279761,00.htm

are all concerned with issues such as the impact of piracy on profits, and are keen to extend the life of copyrights and patents, thus profiting from royalties and licensing agreements by creating more or less permanent enclosures over cultural property.

The TRIPS agreements cover patents, industrial design, trademarks, geographic indicators and appellations of origins, layout design of integrated circuits, undisclosed information on trade secrets, and copyrights (literary, artistic, musical, photographic, and audiovisual).

TRIPS favours industrialised countries and trans-national copyright industries, while limiting the freedom of countries, especially less-industrialised ones, to design IPR regimes to meet their economic, social, and cultural needs. Especially onerous are TRIPS provisions on the patenting of life forms and pharmaceuticals and the appropriation and commodification of indigenous knowledge by international corporations.

19.3. Intellectual property protection and the information society

Intellectual property protection is intended to reward innovation, and to allow people to make money from their ideas. The rules that govern intellectual property are set out in the laws and regulations of national governments, and enforced at the national level. However, the emergence of the global information society has made intellectual property an international issue. Modern information and communications technology (ICT) makes it easy and cheap to copy, modify, and disseminate ideas and information in a wide variety of forms, including audio, video and text. And the global nature of information networks makes worldwide distribution possible in a matter of seconds. In particular, computer technology has made the copyright concept of "tangible medium" less obvious, in that information is so easily heard, viewed, or exchanged without ever taking a physical form. Technological developments have raised copyright enforcement issues as well, largely because it is more difficult to prosecute offenders now due to the speed of technology changes, the volume of infringement, the difficulty in tracking offences across international borders and the decentralised nature of peer to peer networks that copy material.

The worldwide trend is toward harmonization of IP laws and a focus on enforcement, but the views on intellectual property vary widely. Many people support the move toward stronger IP laws that are better enforced around the world, in order to protect the profits of people and companies and foster creativity. They argue that the creator has a moral right to control his own work, and that creators must be compensated for their work, both because that is the ethically right thing to do and because it will help foster a creative society that will bring broad benefits to more people. Others argue that the very nature of information is linked with the concept of sharing and wide use, and that the realities of today's information society demand an entirely new philosophy about intellectual property. They claim that the gains for society when information is shared outweigh the interests of IP owners. They also argue that copyright laws are defective, pointing out that mainstream publishers and music companies make far more profit than creators. Many also question the concept of "originality", suggesting that few ideas are so original that they warrant protection as intellectual property. Also, new thinking on the social value of shared information makes it difficult to impose criminal penalties for copyright infringement where there is no "intent to profit".

'Open' knowledge sharing

New ideas about intellectual property have emerged in recent years that appreciate the importance of creators' rights while at the same time recognising the value to be gained from sharing knowledge and information. The concept of 'open' knowledge aims to create an environment where people share information in order to build on one another's work, but creators get certain rights because of their original contribution.

Free and open source software

Most software that you buy online or in a store is distributed by proprietary software companies that have a copyright giving them the exclusive rights to publish, copy, modify, and distribute the software. They make most of their money by selling an "end user license" to people who use the software programme on their computers. The end user license agreement limits the way you can use the software – for example, only allowing non-commercial uses – and it often restricts you from sharing the software programme with anyone else. You usually agree to these terms either by opening the software packaging (a 'shrink wrap' license), or by clicking "I agree" in a license window that appears when you install the software on your computer (a 'click' license).

Proprietary software companies do not allow the modification of the underlying programming code for the software, the 'source code'. The programming code in which the software is written must be compiled or converted to a form, which will run efficiently on the computer, before it is distributed to the user. In this process the original code becomes inaccessible. If you had access to the source code you could copy, recreate or modify how the software works, and that would allow you to make a similar application very easily (assuming you are a software programmer, or can pay or persuade one to do the work for you!). Access to the source code would also allow

Digital Millennium Copyright Act of 1998 (DMCA)

Under the DMCA, a corporation may do many things not traditionally protected in the USA, such as legally destroy materials a person has bought from them, deny a person's right to sell their used copy of a published work, deny a critic or academic access to the material, or, as has happened in this case, silence and imprison people who point out exploitable flaws in their software.

Not only is this not traditional copyright law, but it is unconstitutional and harmful to the nation, allowing a programmer or company to effectively decide what is illegal or not, allowing industry associations to circumvent the First Amendment rights of individuals, and making security experts afraid to report on their findings.

The DMCA is a law written by a corporation-friendly Congress (H.R. 2281 - 105th Congress) for the benefit of massive corporations with the approval of their lobbying groups like the Recording Industry Association of America (RIAA), the Motion Picture Association of America (MPAA), and the Association of American Publishers (AAP), all of whom support the arrest of Dmitry Sklyarov. The stated intention of the law is to protect the artists' copyright under international treaty. The result has proved something very different.

Some examples:

- Used booksellers and libraries are under direct threat by these measures, and, as reported in the *Washington Post* (February 7, 2001; Page C1), the AAP is actively trying to close them out of the electronic book business entirely.
- Professor Felten of Princeton University cannot discuss his paper on a proposed CD standard for fear of retaliation by the RIAA.
- Links on the web to a code written by a Norwegian minor by the name of Jon Johanssen to allow DVDs to be played on unsupported computers were declared illegal.
- Dmitry Sklyarov, who helped to create software that allows the legitimate owner of Adobe Systems Inc.'s brand of "electronic book" (e-book) files to convert them into generic files, was arrested under the provisions of the DMCA on July 16 , 2001, in Las Vegas, Nevada, where he was speaking to a computer security conference on the techniques Adobe uses in their e-books. His company won its court case.

Source: Campaign for Digital Rights, http://ukcdr.org/issues/sklyarov/

Ruben Blades puts his music on the internet for free

The singer and actor Ruben Blades has put all his latest songs on the web. Anybody can download them for free, and give a donation if they wish. Said Blades: "Send us afterwards what you think is fair for the work done. This experiment will determine whether in the future we can get rid of the middleman and offer our works more cheaply, making sure the profits go directly to the artist."

Source: *Ciberpais*, 31st July 2003, p. 6

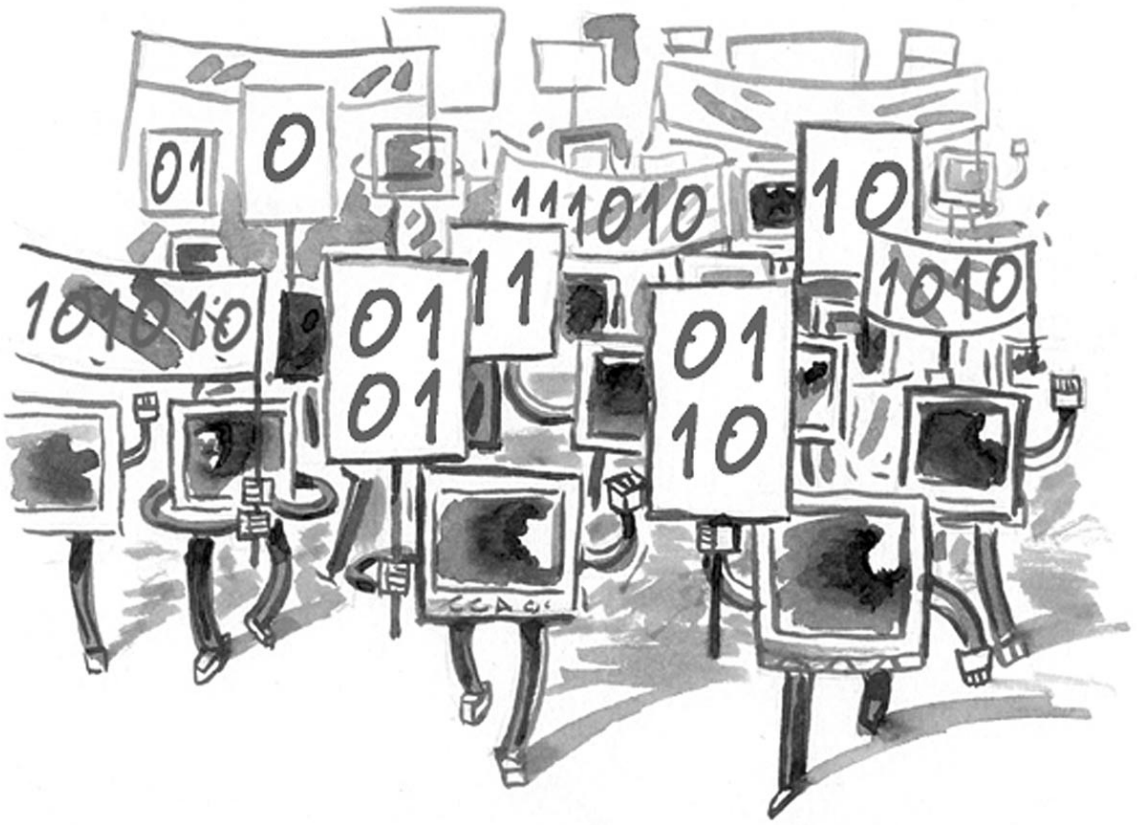
you to make unlimited copies of the software programme (for example, by enabling you to circumvent the built-in copy prevention mechanism). So proprietary software companies keep the source code secret, and they build security mechanisms into the software that prevent you from circumventing the end user agreement. Usually, no one ever has access to see how the source code works. When other people want to make compatible software programmes that will work with the proprietary software, the copyright owner will tell them only what they need to know about how the programme works.

Perhaps the best-known examples of the new thinking about intellectual property are open source and free software. Open source software is software that is made publicly available with the source code open for other programmers to look at. When programmers can read, modify, and redistribute the source code for a piece of software, the software evolves as people improve it, adapt it, and fix bugs. The creator of an open source software application holds the copyright for his work, but distributes the software under a license that grants a number of substantial rights to the user.

Free software has specific social objectives, and uses a form of a license based on four freedoms:

- The freedom to use the software freely. The user has the right to install and use the software on any and as many computers as he likes and use it for professional or private purposes or both.
- The freedom to modify the software to suit the user's needs. The user has the right to change how the software works, can extend its functionality, fix bugs or combine it with other software applications to fit specific needs.
- The freedom to have access to the source code to exercise the right to modify the software.
- The freedom to redistribute the original or modified software, either at no cost or for a fee.

The term 'free software' is not used to indicate that the software costs nothing. In fact, free software is often sold, as in a 'distribution' of GNU/Linux such as Red Hat or SuSE. The 'free' in 'free software' refers to freedom, not to money. Open source does not only refer to the ability to access the original code, although this is the obvious interpretation, and one which some of the more commercial users of the term prefer. Free software is developed by a huge community of programmers, testers, translators, etc, all collaborating via the internet, largely without receiving payment. It thus poses a challenge not only to the proprietary software companies' products, but also to their way of producing commodities, their business practices and their forms of organisation.



The debate around free versus proprietary software

Microsoft Windows and Office proprietary software comes pre-bundled with most new personal computers and has a market share of just over 90% of the world market. Microsoft's Word, Excel and PowerPoint products have become synonymous with text documents, spreadsheets and presentations, and are standards for the electronic exchange of information. The ability to use basic Microsoft products is a valuable skill in almost every occupation and often is required by employers. Proponents of Microsoft Windows and Office proprietary software claim that businesses and individuals that cannot use Microsoft Office applications are clearly at a disadvantage in today's computing environment, because of their widespread use. Training and user support for Microsoft applications is widely available around the world. In addition, the enormous user base makes it easy to find informal help from friends or co-workers. On the other hand, critics argue that Microsoft products are expensive, involve frequent upgrades, and require increasingly powerful equipment to run. Moreover, some complain that the software is too complex, unreliable, and insecure. Another argument is the criticism of the dominant position of Microsoft in the software market, which allows it to dictate to consumers, impose its own criteria and determine trends in software development and thus computer usage. Microsoft' s monopolistic practices have been challenged in the courts in both the USA and the EU. A free alternative to Microsoft will break this monopoly and encourage diversity, improving standards and services.

Once confined to technically advanced users, free software applications such as the GNU/Linux operating system have entered the mainstream market and are today used in many sectors of industry and services on back-end server computers as well as desktop workstations. Proponents argue that free software is an ideal solution for developing countries because it can run on low-end hardware, is easy to maintain and very secure, and unlike proprietary software, free software comes with the per-

mission for anyone to use, copy, and distribute it, usually free of charge. So a country such as China can create its own versions of GNU/Linux, tailor-made to the special needs and conditions of that country. Having the source code means that any suspicions that spyware programmes have been inserted into the programme can be excluded by checking the code. The previous difficulties in installation and hardware recognition have been overcome, although some problems still exist with peripheral devices.

A major distinction of free software is the user's ability to modify the software code. The free school of software development argues that this leads to better software products, which can be developed in less time. Proponents of proprietary software argue that the open source success is based on a non-sustainable business model, only possible because of indirect funding through universities and tax money. Both open source and proprietary software proponents claim that their software development model will foster a domestic software industry in the long-term. The impact of the freedom to modify the source code on users' attitude towards technology has not been investigated enough to indicate if it will lead to more and better computer scientists or not. However, the growing free software movement, and the quality of many free software applications that already exist, indicate that it must be taken seriously as an alternative to proprietary software. Already, developing countries such as Brazil, China, and India, are adopting GNU/Linux as a major alternative to dependence on the Microsoft monopoly.[5]

MIT OpenCourseWare programme

In the educational environment, open content enables the modification and re-use of teaching and learning materials. Coursework that is published as open content can be used at no cost by anyone. The Massachusetts Institute of Technology (MIT) has decided to support open content creation and started a pilot programme to publish its coursework under the "creative commons" license. Its OpenCourseWare programme will eventually make the teaching materials for all MIT courses available free of charge on its website.

Source: http://ocw.mit.edu/index.html

5 http://www.oneworld.net/external/?url=http%3A%2F%2Fnewsforge.com%2Fnewsforge%2F02%2F07%2F03%2F160255.shtml%3Ftid%3D51, http://www.maailma.kaapeli.fi/FLOSSReport1.0.html, http://asia.cnet.com/newstech/applications/0,39001094,39148863,00.htm, http://asia.cnet.com/newstech/systems/0,39001153,39154481,00.htm

Open content

While open source deals with software, open content brings the same approach to a range of other creative works, such as websites, music, film, photography, literature, and learning materials. In this case, the creator has a copyright on the work but allows its use by others under an open content license. There are several widely used licenses that differ somewhat with regard to the rights they grant a user and the protection for the creator, but they stem from the same ideas, and originally found their inspiration in the GPL software licenses (copyleft). Generally the users are allowed to copy, publish, and redistribute the work as long as the original author is given credit, and to modify the work as long as all modifications are clearly marked as such. The supporters of open content believe that free availability of content for others to use, modify and distribute will allow people to work collaboratively and build on each others' work to contribute to a greater body of knowledge, while at the same time reducing duplication of effort.

The Public Library of Science (PLoS) is a non-profit organisation of scientists and physicians committed to making the world's scientific and medical literature a freely available public resource

The internet and electronic publishing enable the creation of public libraries of science containing the full text and data of any published research article, available free of charge to anyone, anywhere in the world. Immediate unrestricted access to scientific ideas, methods, results, and conclusions will speed the progress of science and medicine, and will more directly bring the benefits of research to the public. To realize this potential, a new business model for scientific publishing is required that treats the costs of publication as the final integral step of the funding of a research project. To demonstrate that this publishing model will be successful for the publication of the very best research, PLoS will publish its own journals. *PLoS Biology* is accepting submissions now, and the first issue will appear in print and online in October 2003. *PLoS Medicine* will follow in 2004. PLoS is working with scientists, their societies, funding agencies, and other publishers to pursue our broader goal of ensuring an open-access home for every published article and to develop tools to make the literature useful to scientists and the public.

Source: http://www.publiclibraryofscience.org/

Creative Commons

Creative Commons is a non-profit corporation founded on the notion that some people may not want to exercise all of the intellectual property rights the law affords them. We believe there is an unmet demand for an easy yet reliable way to tell the world 'Some rights reserved' or even 'No rights reserved.' Many people have long since concluded that all-out copyright doesn't help them gain the exposure and widespread distribution they want. Many entrepreneurs and artists have come to prefer relying on innovative business models rather than full-fledged copyright to secure a return on their creative investment. Still others get fulfillment from contributing to and participating in an intellectual commons. For whatever reasons, it is clear that many citizens of the Internet want to share their work – and the power to reuse, modify, and distribute their work – with others on generous terms. Creative Commons intends to help people express this preference for sharing by offering the world a set of licenses on our Website, at no charge.

Our first project is to offer the public a set of copyright licenses free of charge. These licenses will help people tell the world that their copyrighted works are free for sharing – but only on certain conditions. For example, if you don't mind people copying and distributing your online photograph so long as they give you credit, we'll have a license that helps you say so. If you want the world to copy your band's MP3 but don't want them to profit off it without asking, you can use one of our licenses to express that preference. With the help of our licensing tools, you'll even be able to mix and match such preferences from a menu of options. **Attribution:** Permit others to copy, distribute, display, and perform the work and derivative works based upon it only if they give you credit. **Noncommercial:** Permit others to copy, distribute, display, and perform the work and derivative works based upon it only for noncommercial purposes. **No Derivative Works:** Permit others to copy, distribute, display and perform only verbatim copies of the work, not derivative works based upon it. **Share Alike:** Permit others to distribute derivative works only under a license identical to the license that governs your work. .... If you prefer to disclaim all ownership – in the footsteps of innovators ranging from Benjamin Franklin to modern-day software pioneers – we'll help you do that, too. You can dedicate your work to the pool of unregulated creativity known as the public domain, where nothing is owned and all is permitted. In other words, we'll help you declare, 'No rights reserved.'

Source: http://creativecommons.org/faq#faq_entry_3311

Patenting of ideas and software

Although patents have been allowed on ideas and software, traditionally there have been restrictions on this, which meant that patents were granted mainly on inventions of physical things. Recent interpretations of the patenting laws in the USA have led to in increase in software patents. Instead of the code from a computer programme being protected by copyright, similar to a literary work, it is treated as if it were a technological invention. There are two main problems here.

First, any one programme will always use many different sub-programmes, and some of these may be patented already. So software patents can make software copyright useless. As more and more software ideas are patented, to find out if your programme uses already patented ideas will be extremely costly or impossible. One copyrighted work could be covered by hundreds of patents and the author could be sued for patent infringement without even knowing that he/she is using those patented ideas. This situation will make software programming extremely costly, and only the lawyers will be happy. Small companies will find it increasingly difficult to support the cost of the necessary legal advice.

Second, software patents are extremely broad, because they cover ideas, not concrete ways of doing or making things, so basically anything is patentable. For example, a traditional patent could be of a technique for making buttonholes. But a patented idea could be the concept of a buttonhole. If this seems ridiculous, the truth is sometimes stranger than fiction. Attempts to patent the wheel and all possible telephone numbers were surprisingly successful at first. But Amazon has the patent for one-click purchasing, and prevented its competitor Barnes & Noble from using this idea. It is not a programme they have patented, not a complicated code sequence, but the idea of one-click purchasing.[6] Recently, the European Parliament approved a Patents Directive, which had been amended to exclude software from patenting, in response to a campaign against this.[7]

6 See Boycott Amazon! at http://www.gnu.org/philosophy/amazon.html

7 See http://swpat.ffii.org/, http://news.zdnet.co.uk/business/legal/0,39020651,39116642,00.htm

19.4. Intellectual property protection in developing countries

Overall, intellectual property protection has not been a priority for developing countries until recently. Previously, colonial systems instituted IP regimes that primarily protected the interests of colonising nationals and businesses. IP laws were seen as a tool for foreigners to protect their profits. During subsequent post-colonial periods, there was very little enforcement of intellectual property rights, and counterfeiting, illegal copying, and pirating were common. In some countries, local industries were built around intellectual property violations, such as the infamous software pirating industries of Asia. Many argue that it is OK for developing countries to copy things like music, films and software that come from developed countries because it brings profits to the local economies where it is needed most. Others highlight the costs to local industries and artists that cannot gain IP protection for their work in the domestic market and cannot compete with low cost copies made by others. For example, the lack of intellectual property enforcement in Ghana is said to be responsible for the migration of many Ghanaian recording artists to Europe where their work can be protected.

Previously it has been the case that many developing countries did not have patent laws in place, and this created an environment where people could exploit inventions patented in other countries. Pharmaceuticals and agro-chemicals are two areas where this was a particular issue. The WTO, WIPO and others (notably developed countries where patent holders have a powerful voice) have been urging developing countries to update their patent laws. The US and European pharmaceutical industries argue that patent protection is needed so they can sell their drugs at a price that will allow them to recover the enormous costs involved in drug research and development. They say that developing country governments must enforce their intellectual property rights against locally manufactured generic versions of their drugs that would be sold for far less. IP proponents point out that national patent laws would also help foster domestic drug industries in developing countries, which would attract foreign investment and result in increased employment and exports. Developing countries hold the position that their immediate need for drugs to deal with the monumental healthcare crises they face is a greater priority than intellectual property enforcement for foreign pharmaceutical companies. Many are acquiescing to pressure from international organisations and complying with their obligations under international treaties, but the cases of South Africa, India and Brazil, which threatened to ignore the patents on HIV antiretroviral drugs and produce or import their own cheap substitutes for these drugs, has shown the hollow nature of the pharmaceutical companies' arguments. Coupled with a huge campaign in conjunction with civil society to denounce the immorality of the high prices demanded by the companies for their products, which in practice meant the death of millions of people from AIDS and little or no sales in poor countries, these countries were able to pressure the pharmaceutical industry into accepting much lower prices. This significant victory for developing countries shows that international campaigns can have an effect on industrial sectors that seem omnipotent.

19.5. Indigenous knowledge

Indigenous knowledge is another concept that pushes the boundaries of traditional intellectual property regimes, based on the notion that communities share in the value of the knowledge that they hold as a group because there is no single creator or discoverer of the information. Indigenous knowledge is information and wisdom that is locally held and unique to a particular culture or community, usually within developing countries. The body of indigenous knowledge is often maintained through an oral tradition where knowledge is handed down through the generations via storytelling. Information is usually considered 'indigenous' where it is different from the kind of information commonly learned in conventional educational systems. Rather, indigenous knowledge is gleaned at the local level and emerges from the historical lessons of daily life in the local context. It is not considered to be the property of any one person or group, but rather of the entire community.

There is increasing recognition of the role that indigenous knowledge systems play in development. In particular, indigenous knowledge is being used in the creation of sustainable and environmentally sound approaches to agriculture and natural resource management. It is also being tapped to inform decision-making on food security, healthcare, education, and other areas. There is a growing interest in capturing indigenous knowledge in audio, film and written formats in order to help communities gain intellectual property protections for it. For example, knowledge of local plants that have medicinal value can be recorded and exploited economically for the benefit of the community. This is particularly important in the context of biotechnology and biopharmaceutical industries. And ICT is helping to make indigenous knowledge more accessible and easier to disseminate. For example, as existing indigenous knowledge resources becomes linked, it allows knowledge sharing among communities with similar circumstances in different parts of the world.

Some indigenous people see a need to make a permanent record of this knowledge for future generations, as they believe such generations will be less reliant on traditional ways. And also, it helps to demonstrate their rightful ownership of the land and their own knowledge, which in some cases has been threatened by private companies attempting to patent drugs known by indigenous peoples for many years, or by art dealers who exploit traditional indigenous, sometimes sacred, designs.

Ancient traditions preserved

On Elcho Island, in the north of Australia, aborigines are using ICTs to preserve their traditional knowledge system. They are recording oral traditions, normally passed down in non-written form from generation to generation. The whole variance of their rich cultural tradition will be digitalised to prevent it from being lost and saved in a complex database. The intellectual system of the different clans of the tribe, expressed in words, music, dance and painting will live on in the computers of the Galiwinku Knowledge Centre.

Similar projects are under way, or under consideration, elsewhere in the traditional Aboriginal world: in the Pitjantjatjara lands of Central Australia, where a vast online archive of old photographs and stories has been established; and at Wadeye and Belyuen in the Top End, where old songs have been recorded on digital audio.

Howard Morphy of the Centre for Cross-Cultural Studies explains: "New technology is allowing people to store and access their cultural knowledge. This is part of an emerging shift of great importance."

Source: http://australianit.news.com.au/articles/0,7204,6569260%5e15302%5e%5enbv%5e,00.html

20. Freedom of expression and censorship

Under international human rights conventions, all people are guaranteed the rights to free expression and association. As we shift from communicating using 'physical' formats such as letters, newspapers and public meetings, to electronic communications and on-line networking, we must consider how these rights apply to these new realities. There is no simple and obvious way of extending our existing rights to cover issues that emerge with the use of new technologies. To do that effectively we need to address the specific context within which our rights are to exercised and defended.

20.1. The rights of expression, communication and association

Various international agreements on human rights were drafted immediately after the Second World War. In the context of that time, guaranteeing the fundamental right an individual in society to live, work and participate in the democratic process, according to the rule of law, was appropriate and necessary. Today, the situation within which these rights operate has changed. New information and communication technologies, the Internet in particular, present a challenge, since they allow open communication outside of state regulated and licensed media channels, and beyond national borders. Exactly how Human Rights must be interpreted in this new context has to be established.

The UN Universal Declaration of Human Rights guarantees freedom of thought, expression, association and communication. These have been replicated within regional treaties, such as the European Convention on Human Rights, and many national constitutions. Exercising these rights on the Internet is a complex matter, as it operates beyond national boundaries with no clear legal jurisdiction, in a medium that presents specific technological challenges. For example, although the UN Universal Declaration on Human Rights protects the right to privacy and private correspondence, the monitoring of Internet communications (by employers and service providers) is commonplace. The means of preventing such intrusion (through encryption, for example), are often restricted by governments.

United Nations Universal Declaration of Human Rights [1]

Article 18

Everyone has the right to freedom of thought, conscience and religion; this right includes freedom to change his religion or belief, and freedom, either alone or in community with others and in public or private, to manifest his religion or belief in teaching, practice, worship and observance.

Article 19

Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

Article 20

(1) Everyone has the right to freedom of peaceful assembly and association.

Article 30

Nothing in this Declaration may be interpreted as implying for any State, group or person any right to engage in any activity or to perform any act aimed at the destruction of any of the rights and freedoms set forth herein.

1 Available online from http://www.un.org/Overview/rights.html

Although Article 19 of the UN Declaration gives rights of communication 'regardless of frontiers', in some states, such as China, it is difficult to exercise this right. China attempts to filter all communications going in and out of the country as part of a system that has been described as 'The Great Firewall of China'. The purpose of this system is to restrict the flow of information out of and into the Chinese Internet. This system also forms part of an effort by the Chinese state to restrict Internet content within China, by tracking the use of the Internet for communication, in order to limit dissent on-line[2]. For example, this system has been effective in repressing the spread of information related to the Falun Gong movement[3]. A recent study found that up to 200,000 international web sites may be blocked in China,[4] and China-related matters figure high on the list of 'Internet dissidents' maintained by Human Rights Watch[5].

Vietnam imprisons dissident for using Internet

Pham Hong Son was arrested in March 2002, and charged with spying under article 80 of Vietnam's Penal Code because he communicated by telephone and email with "political opportunists" in Vietnam and abroad.According to the indictment: "Son willingly supported the view of these mentioned political opportunists and became a follower of the action plan to take advantage of freedom and democracy to advocate pluralism and a multiparty system in order to oppose the government of the Socialist Republic of Vietnam." He is also accused of receiving emails from dissidents abroad who said that "the way to change the nature of the current regime was to remove the restrictions imposed by the Party leadership and Government, and to unify and organize the forces of democracy and pluralism."

After a half-day closed trial in Hanoi on June 18, 2003 Pham Hong Son was sentenced to thirteen years' imprisonment and three years of house arrest on espionage charges under article 80 of Vietnam's penal code.

Source: http://www.hrw.org/advocacy/internet/

In less obvious form, restrictions on the content of on-line information, and requirements for the registration or licensing of web sites, also limit the ability of people to express opinions and to communicate freely. This transfers the onus for regulation from the state – which may be challenged in the courts – to the private companies that run Internet and communications services. In order to maintain their licensing, or to prevent crippling lawsuits, these companies 'self-regulate', deciding what is or is not acceptable. Challenges to such decisions are often not feasible, and are ultimately controlled by carefully crafted 'terms of use' that users must agree to before they are allowed to use the service.

Perhaps the greatest obstacle to free expression of views (even views that do not violate laws on hate speech or the promotion of violent or unlawful acts) is the standard contract that users must agree to when signing up for an Internet service. Often we must give up our rights in order to have access to electronic networks. Most standard contracts include conditions related to defamation and the 'misuse' of electronic networks. For example Microsoft Network's (MSN's) contract[6] states that users should not,

- Defame, abuse, harass, stalk, threaten or otherwise violate the legal rights (such as rights of privacy and publicity) of others.
- Publish, post, upload, distribute or disseminate any inappropriate, profane, defamatory, obscene, indecent or unlawful topic, name, material or information.
- Upload, or otherwise make available, files that contain images, photographs, software or other material protected by intellectual property laws, including, by way of example, and not as limitation, copyright or trademark laws (or by rights of privacy or publicity) unless you own or control the rights thereto or have received all necessary consents to do the same.

These terms represent conditions that interpret the standard laws on defamation, privacy and intellectual property that exist in most states. However, the contract gives the operator the right to limit or discontinue access to the service without requiring evidence that the user has committed any unlawful act, or has actually transmitted material that could be deemed defamatory by a court of law. It is Microsoft's interpretation of the facts of the case, which is applied without consideration of the specific details and requirements of each. The contract that users must agree to also ensures that any challenges to the terms of the contract must take place in Microsoft's local court:

"Microsoft reserves the right, in its sole discretion, to terminate your access to any or all MSN Sites/Services and

2 See information on China from Reporteurs Sans Frontiers – http://www.rsf.fr/chronicle.php3, http://www.rsf.org/article.php3?id_article=6793

3 See http://www.clearharmony.net/cat/c1134/c1134.html

4 The commentator John Naughton carried out a review of the study for The Observer – see http://www.observer.co.uk/business/story/0,6903,855769,00.html

5 See the Human Rights Watch web site – http://www.hrw.org/advocacy/internet/and http://www.hrw.org/advocacy/internet/dissidents/

6 Available via Microsoft's Networks' web site – http://www.msn.com/

the related services or any portion thereof at any time, without notice... Claims for enforcement, breach or violation of duties or rights under this agreement shall be adjudicated under the laws of the State of Washington, without reference to conflict of laws principles... You hereby irrevocably consent to the exclusive jurisdiction and venue of courts in King County, Washington, U.S.A. in all disputes arising out of or relating to the use of the MSN Sites/Services."

The ability of a service provider to use its discretion to remove access to services (and hence limit expression), without bothering with legal procedure, is a violation of rights. It allows service providers, whether on their own initiative or following pressure from government or industry organisations, to violate the rights of individuals who wish express their views on the internet, even when there is no lawfully based reason to curtail their use of that service. This places the control and interpretation of human rights in private hands, outside legislative regulation.

For organisations using Internet services it is important to evaluate the conditions of the service contract, and their potential to restrict rights of expression, before taking up any service. The conditions placed on email or web services vary from provider to provider. Other factors, such as the level of data protection in the country where the service operator is based, are also important. Gaining Internet access, in order to upload information over the 'Net to a service, is fairly straightforward, and does not usually create problems. It is the conditions on hosting that most affect groups and individuals. For this reason those who wish to run on-line services that support or provide information on contentious issues should seek out service providers, perhaps in more than one country, in order to ensure that the information they host cannot be easily taken down.

Privacy policies are another issue. Most commercial sites have a privacy policy, but liberally interpret it in certain circumstances. For example ebay, the online auction site, has been happy to hand over private information to law enforcement agencies without any official court order[7]. According to one ebay executive:

"When someone uses our site and clicks on the 'I Agree' button, it is as if he agrees to let us submit all of his data to the legal authorities. Which means that if you are a law-enforcement officer, all you have to do is send us a fax with a request for information..."

ebay also owns the 'PayPal' online payment system, and have reputedly been willing to disclose to the authorities credit card data from user accounts on that site. This can be seen as part of a wider agenda to develop standard procedures that would give the state access to information kept by Internet service providers. Moves to formalise this relationship have been made in various International forums, in particular via the G8 conference[8].

For those who have the resources, challenging the restrictions on access to on-line material may prove a useful way of protecting rights to expression and communication. To date, some of the leading challenges to new forms of on-line censorship have been launched by groups in the USA such as the American Civil Liberties Union (ACLU) and the Electronic Frontiers Foundation (EFF – which also has similar organisations based in other states). Other organisations, such as the Association for Progressive Communications (APC), have also instituted projects to track and report cases involving censorship and restrictions of rights on-line[9]. For those wishing to campaign on rights of access, these organisations provide a good model for planning similar actions[10].

20.2. Censorship and technical restrictions on network access

Censorship is the means by which states have sought to restrict the transmission of information. Information is blocked either by legal restrictions on content, or by requiring the licensing of service providers. Unlike other media, such as radio, TV and newspapers, the Internet is far harder to license. This is because if threatened the operator can move to another state where licensing restrictions are less severe, though some states seek to control not the source or transmission route of the information, but its reception by the user. This is achieved by requiring the fitting of software systems to computers or access terminals that restrict the information a person may receive.

The technical systems that can be used in computers, or by internet service providers, provide a simpler and more effective means for controlling access to material. These software systems become an indirect form of state censorship. Two main types of system are currently available[11]:

7 See Haaretz Daily, 10th august 2003, 'Big Brother is watching you - and documenting'.

8 See information on G8 Government/Industry Conference on High-Tech Crime Tokyo, May 22-24, 2001. Information on G8 summits is held, at various levels of detail, by the foreign ministries of different states. *Report of Workshop 2 – Data Preservation* is available via the Japanese Foreign Affairs Ministry web site – http://www.mofa.go.jp/policy/i_crime/high_tec/conf0105-5.html

9 The APC monitoring projected is centred on three regions: Latin America and Caribbean ICT Policy Monitor – http://lac.rights.apc.org (in Spanish); Africa ICT Policy Monitor – http://africa.rights.apc.org (in English)
Europe ICT Policy Monitor – http://europe.rights.apc.org (in English)

10 ACLU – http://www.aclu.org/ EFF – http://www.eff.org/

11 There is an excellent database of resources on filtering and blocking software maintained by the Electronic Frontier Foundation – http://www.eff.org/pub/Net_info/Tools/Ratings_filters_labelling/

- *Filtering* – sifting the packets of data or messages as they move across computer networks and eliminating those containing 'undesirable' material; and
- *Blocking* – preventing access to whole areas of the Internet based upon a 'blacklist' of certain Internet address, locations or email addresses.

Tests on Commercial Filtering Software

Jamie McCarthy tested commercial filtering software that, according to the manufacturer, is used in 17,000 schools (more than 40% of schools in the USA). The researchers found that the software filtered educational, cultural, historical and political information on many web sites which did not contain sexually explicit material, including the following:

Campaign Finance Reform Talking Points.

ECM Publishers. (not pornographic publishers)

How a Bill Becomes a Law. A brief lesson plan for teachers, to help them explain the legislative process to their students. Includes links to valuable net resources.

The Traditional Values Coalition, "the largest non-denominational, grassroots church lobby in America." Ironically, their homepage currently has a strong statement supporting the use of blocking software in our schools and libraries.

Pennsylvania Rules of Criminal Procedure.

American Government and Politics, a class taught at St. John's University by Dr. Brian L. Werner.

The Circumcision Information and Research Pages, an activist and research site which contains no nudity and has won the "Select Parenting Site" award from ParenthoodWeb.

Source:http://www.epic.org/censorware/mandated_mediocrity.html

Filtering operates on the basis of 'rules' that target certain words, phrases or colour combinations in pictures. When the conditions of a rule are met some type of action is triggered. The rules are usually applied as part of the computer program accessing the information, either at the 'socket' where the computer accesses the network, or at the server that routes the information across the Internet. This type of filtering tends to be very crude, because the rules operate without taking account of the context in which the offending term is being used. Many filtering programs, which are often used in public libraries, schools and other public terminals, can obstruct requests for completely inoffensive material.

Blocking usually uses a database of restricted web addresses or email servers. When an attempt is made to access a blocked site the request is refused by the browser, or the packets or messages are blocked at the network socket or server. A request will also be denied if material is requested from a blocked site as part of another web page.

There are technical differences in how rules for filtering or lists of blocked sites are determined. Rules based systems (filters) can usually be manipulated by the user, who can make choices as to which words or conditions to filter and can turn filters off or on, although many systems have a default set of words that are configured automatically. Most blocking systems do not allow the user control over the content of the database itself (although addresses may be added to the database). Instead the user must accept the selection criteria used by those who control the system. Finding out which sites are blocked can also be problematic. The database of a blocking system is usually encrypted to prevent access to its contents; this makes it an 'intellectual construct' under intellectual property law, and any attempt to decrypt its content, in order to obtain a list of blocked sites can result in prosecution by the creators of the software involved.

Concerns have been raised about the use of blocking and filtering software and their impact on freedom of expression. In the USA, where blocking and filtering systems are widely used, investigators have found that a wide range of sites are blocked, not merely those deemed 'offensive' because of their sexual or violent content[12]. For example, some sites with a sexual, but not pornographic, content, such as gay and lesbian rights websites, may also be blocked. Increasingly sites are blocked on the basis of their political content. Some studies have found that whilst certain 'offensive' hate sites are blocked, sites (including some belonging to religious groups) which contain other forms of hate speech, are not blocked.

12 See the EPIC report, *Faulty Filters: How Content Filters Block Access to Kid-Friendly Information on the Internet* –http://www.epic.org/reports/filter-report.html

Note also that most of the current 'spam filters', that seek to restrict spam emails a user receives, can also use blacklisting systems in addition. These blacklists are maintained by certain companies who study recent spam incidents, and the filter programs update their blacklist database over the 'Net at regular intervals. This means that when an email relay is hijacked by spammers, the users of that email service may find their emails are blocked. It is also possible that rules-based anti-spam systems may specifically restrict emails from certain named sources.

A new form of censorship has emerged recently with allegations that Internet search engines are being manipulated to block the inclusion of certain web sites. If the search engines can be configured not to include references to certain sites then access to those sites is effectively blocked off because 'Net users will be unaware of their existence. A recent example of this was the allegation by the Bilderberg.org site[13] that its entry in *Google* had been removed in order to prevent information about the Bilderberg Conference (a private conferences of politicians and leading corporations) being distributed.

For those concerned about the impact of filtering or blocking software, the easiest option is to demand from the software developer details of the criteria for the rules set or blacklist. However, most developers of these systems refuse such requests on the basis of 'commercial confidentiality'. Some groups have proposed the development of an 'open source' content filtering system, so that all the rules and blacklists used by the system would be open to scrutiny. But as yet there is no specific project by the open source community to develop a system for used by ordinary computer users.

13 See http://www.bilderberg.org/legal.htm

Those worried that their services may be blocked by software systems, should obtain copies of recent versions of blocking or filtering systems and attempt to access their services on-line. Likewise, to ensure that their sites are appropriately listed in search engines, they should regularly search for information on their web sites using a number of the leading search engines.

Finally, there is one critical factor about the use of electronic networks and censorship. Because the operation of the network is largely beyond the control of the users, the network may be censored, technologically or manually, by those who design, install or operate the system. Likewise, any technological system is open to abuse by those who are able to exploit flaws in the network. A good example of this is the hacking or blocking of sites. This may be done unofficially – for example the blocking of access to the Al Jazeera TV network web site during the Gulf War[14] – or officially – for example, the Presidential Order signed by George W. Bush that allows the US to conduct 'cyberwar' against another state[15].

20.3. Defamation actions as a means of silencing criticism

'Defamation' involves the publication of a statement damaging a person's reputation. A company or individual may use the threat of a defamation action to silence their critics or campaigners. There have been many examples of this, even before the Internet was a popular communications medium for civil society campaigns[16]. Internet service providers, like other publishers, will not normally defend against a claim of defamation. Rather than risk the costs involved in a legal action, many will simply remove the offensive material and undertake not to allow its future publication. Where a claim of defamation is made against the originators of the information or statements they must decide whether to fight the action, because they believe their claims are correct, or to apologise and risk a claim for damages.

The most famous example of such a case, which saw ground-breaking use of the internet, was the McLibel Trial[17]. In a defamation action by McDonald's against Greenpeace London, two of the defendants used the court case as a campaign opportunity. How the McLibel two took on the McDonald's corporations is a good example of how to handle threats of legal action.

14 See a report on the Al Jazeera attack from News.com – LINK http://news.com.com/2100-1002_3-1016447.html?tag=fd_top

15 See the Washington Post, 7th February 2003, 'Bush Orders Guidelines for Cyber-Warfare' – http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A38110-2003Feb6&notFound=true

16 A good account of corporate legal action against campaigners is contained in Andrew Rowell's book *Green Backlash* - see reference 1 above.

17 McSpotlight - http://www.mcspotlight.org/

21. Privacy and security

'Privacy' is something that is difficult to define because it is a subjective matter. Some people have a wish, for personal reasons, to move through society anonymously, without interference in their affairs. Others have no problems giving out information about themselves in order to access information, goods or services. For most people, privacy is an issue of simplicity and security. People like to access services without complicated forms and reference checks, and may be willing to allow information systems track their movements or purchases.

Security is closely related to privacy. A secure information system does not disclose information when it is not appropriate to do so. The disclosure of information is not a neutral act. People collect, or process information for a purpose. It is the intention of those who collect personal information, or who trade it and put it on a database, to create profiles of individuals for certain purposes. How we mange the disclosure, use and storage of personal information will decide whether information technology become a source of empowerment or of repression.

In considering how privacy is measured and protected, we must distinguish between different types of privacy:

- For most people, privacy means 'personal privacy' – the right of individuals not to have their home, private life or personal property interfered with. This can be considered as 'real world' privacy.
- A related aspect of this is 'bodily privacy' – the right of individuals to protect themselves from medical or genetic testing, and to have information about their health or personal well-being protected by those with access to such information (doctors, employers, insurers, etc.).
- 'Privacy of communications' refers to protection from interference with communication over the phone or the internet. Respect for the privacy of communications is an essential prerequisite for the maintenance of human relationships via technological communications media.
- 'Information privacy' is perhaps the most widely debated aspect of the use of computers and information systems. Information systems are able to hold and process information about large numbers of people at high speed. It is important to ensure that information will only be used for the purposes for which it was gathered, and that it will not be disclosed to others without the consent of the relevant individuals.

Privacy threats on the web

When you are surfing the web you may think you are anonymous, but there are various ways that information about you or your activities can be collected without your consent:

- Cookies
- HTTP
- Browsers
- There may already be information about you published on the web
- Downloading freeware or shareware
- Search engines
- Electronic commerce
- E-mail
- E-mail and cryptography
- Spam
- Dangers of Internet Relay Chat

Source: "Protecting your Privacy on the Internet", Australian Privacy Commissioner, http://www.privacy.gov.au/internet/internet_privacy/index.html

The Code of Fair Information Practices

The Code of Fair Information Practices was the central contribution of the HEW (Health, Education, Welfare) Advisory Committee on Automated Data Systems. The Advisory Committee was established in 1972, and the report released in July. The citation for the report is as follows: U.S. Department of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records, computers, and the Rights of Citizens viii (1973).

The Code of Fair Information Practices is based on five principles:

1. There must be no personal data record-keeping systems whose very existence is secret.
2. There must be a way for a person to find out what information about the person is in a record and how it is used.
3. There must be a way for a person to prevent informa tion about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.
4. There must be a way for a person to correct or amend a record of identifiable information about the person.
5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.

Source: http://www.epic.org/privacy/consumer/code_fair_info.html

21.1. Legislative frameworks for protecting privacy

There are different legal frameworks for the protection of privacy. The legislative framework of most states deals with information privacy and to a lesser extent with bodily privacy. The protection of personal privacy is usually a civil matter. This means that infringements of privacy must be contested by individuals in the courts, and the state will not act on their behalf.

In some states, individuals are wholly responsible for monitoring their privacy, and seeking legal redress when it is infringed. The problem with this model is that if individuals do not have the means to police their privacy, such as the financial security to bring a case to court, then they have no privacy. In other states, the burden for protecting privacy is placed on the holder of the information. Although this takes the burden off the individual, it can also lead to a false sense of security because it is assumed that the holders of the information, or the regulatory bodies that are set up to police them, will protect interests of the individual.

The region with the strongest information privacy laws is the European Union. Following the introduction of various laws in the 1980s and 1990s on the protection of personal data[1] there is now a strong framework to protect the information held on computers. Over the next five years, this legal framework will also be extended to certain types of paper-based records. To back up the legislative framework, each state in the EU also has its own agency, with legal powers, to police the holding of personal information. Holders and processors of personal information must obtain a permit from this agency.

The approach of the European Union contrasts with that of other states such as the USA and Singapore. These states primarily opt for self-regulation within different sectors of industry, or they legislate very narrowly to protect only certain aspects of personal privacy. In the USA especially, the structure of privacy laws means that information held by bodies other than the state is open to be used and traded by anyone, unless a law specifically exists to protect it.

The problem with self-regulation is that it addresses the needs of the data processing industry rather than the interests of the individual. Codes of practice that create 'burdens' on organisations, or affect their ability to trade or operate, may only be grudgingly implemented. The lack of any transparency in the application of such codes also makes it difficult to establish that they are properly applied in all cases. These systems are also subject to 'functional creep', as new processes are added that are not specifically controlled by self-regulation procedures. This is significant in the context of the Internet. The sale of personal information is, for many Internet companies, a major income stream. As new on-line services have developed so the opportunities for the gathering and trading of personal information have increased.

With regard to communications privacy, the introduction of digital communications, whilst enabling a boom in cheap telephone and computer-based communications, has at the same time lessened the protection for personal communications. While the content of our communications is secret, unless intercepted by the state, the collection and retention of traffic data represents a less serious but still damaging invasion of privacy. The potential uses of retained communications data, and its value when forming data profiles on individuals, has not received

1 For a review of data protection in the European Union and related issues see http://www.internetrights.org.uk/

wide public attention – even though data retention forms the core of the measures enacted as part of the so-called 'war on terrorism'.

For those interested in protecting their privacy, the simplest advice is to meet their needs for information services in states that have strong data protection laws. This may be very difficult for people who are not residents in such states, though. At the same time people should seek to restrict the information that they give out about themselves as part of consumer surveys, or in response to purchases at stores.

Organisations should be careful with the way they process personal information. The impact of junk mail, faxes and text messages has led the public to develop a negative perception of organisations that trade or sell personal data. For those organisations that are involved with political or social causes, the protection of personal data is increasingly important given recent legislative changes on data retention. If data is not held securely, and transmitted securely, then the organisation risks disclosing information about its supporters or partners.

Human Rights Activists in South Korea start Hunger Strike against National Education Information System (NEIS)

"NEIS - A giant digital database established by the government to gather the private information of students, parents, and teachers" * [Press Release] People requests to halt the implementation of NEIS immediately

Seoul, South Korea – June 18th, 2003, nine human rights activists in South Korea starts hunger strike struggle on the street against National Education Information System (NEIS) for an indefinite period. They stressed that NEIS, which is a giant database of people's private information, is to infringe basic human rights including privacy very seriously, and requested that the government should halt the implementation of NEIS and delete the section of private information in NEIS. They also condemned that the government is trying to gather lots of private information into this system without any agreements from people, so it is absolutely illegal and unconstitutional.

Korean Progressive Network(Jinbonet), Sarangbang group for Human Rights, Center for Human Rights Dasan, Peace & Human Rights Coalition, Chunbuk Peace & Human Rights Coalition, Catholic Human Rights Committee, and Minkakyup Human Rights Group, Won Buddhism Human Rights Committee participate in this hunger strike struggle.

Source: Copyleft by www.base21.org

21.2. Privacy enhancing technologies (PETs)

The development of digital communications technologies has improved our ability to communicate. But we do so at the cost of generating a long trail of information. For people dealing with sensitive information who must avoid disclosure, or who need anonymity, communicating presents new challenges. However, alongside the development of digital communications, there has been a parallel development of systems that allow communication to take place more securely. These are collectively known as 'privacy enhancing technologies'.

In the mainstream, some internet-based services have sought to develop privacy within information services. The World Wide Web Consortium (W3C) has recently developed a 'Platform for Privacy Preference's (P3P)[2]. This works within the user's Web browser, and for those sites that are P3P compatible. The user's privacy preferences are communicated to the web server as part of web browsing, or submitting information to web sites. This enables those gathering information to know precisely how to deal with the information gathered from Web users.

In relation to on-line trading, systems have also been developed to allow people to have an on-line method of verifying their identity. The leading system at the moment is Microsoft's *Passport* – although it has been plagued by problems related to the unintended disclosure of personal information. These systems work by establishing a verifiable identity that can be securely accessed by internet servers, rather than requiring you to submit information such as passwords yourself. However, like P3P, Passport is a system for secure information *sharing* rather than for allowing users to supervise the information that is gathered and held about them by a particular on-line service.

Systems that actively protect privacy have been promoted by independent software developers. There are two general types of systems:

- Systems that use encryption to secure the content of the communication, or that use encryption to digitally sign information to prove its authenticity;
- Systems that use a proxy – the forwarding of information on-line without creating traffic data – in order to prevent the disclosure of its true source.

A large number of options are available for improving privacy on-line. They generally rely either on using a proxy or on encryption/digital signatures. Details can be found in a document developed by the Association for Progressive Communications, as part of a project with civil society groups, entitled 'Participating With Safety'[3].

2 See the W3C's *Platform for Privacy Preferences Project* (P3P) overview – http://www.w3.org/P3P/

3 The *Participating With Safety* materials are available at http://secdocs.net/manual/lp-sec/

By using a proxy system the source of an on-line communication can be disguised. A proxy server erases all information that discloses the source of a message or packet and then forwards the packet onto its destination using its own identity. On receipt of a reply, it replaces the correct identity of the requesting address, and returns it. In this way the 'chain' of data retention between the user and a server is broken. However, care must be taken to ensure that the proxy used is trusted and secure.

Various types of proxy services operate on the internet[4]. If the proxy server keeps no logs, it can disguise the source of the data, though most commercial services keep logs to allow tracing should there be any legal queries about a particular data transaction. The few proxies that keep no logs, and operate in a truly anonymous manner, are at risk of legal actions undertaken by parties offended by the information that gets relayed through them. Most of the anonymous proxies have closed. Others often operate for a short time before closing down to avoid legal action. Many states have begun to enact laws that require communication information to be collected, stored, and turned over to authorities upon request, and it is becoming more difficult to find a legal jurisdiction where a proxy server may operate.

Encryption systems are a valuable tool to preserve privacy and confidentiality. Built-in encryption systems, like the 'secure shell' function in web browsers, and some weak encryption systems like those that scramble your word processor file with a password, are considered acceptable. But many states have now legislated to control the use of strong encryption systems, like those used to generate digital signatures or to scramble documents for transmission over the Internet. Each state has a slightly different legal requirement. Some states, like the Russian Federation, will not allow encrypted material to be brought into the country. Some, like Ireland, allow encryption to be used, but in case of legal action you must produce an unencrypted copy of any document requested. The UK, like a number of other states, requires that in the case of a police investigation you turn over all your encryption keys and passwords or face prosecution.

In a system where data flows are 'open' to anyone able to intercept them, encryption is the only means of guaranteeing the privacy of the communication. Encryption is the only guaranteed method of protecting sensitive information from disclosure if your computer is lost or stolen. Therefore it is essential that the right to encrypt information remains. If we cannot use encryption because it is legally banned, the public will suffer. Those who wish to break the law will continue, for their own reasons, to encrypt and hide their data to prevent disclosure.

Another useful implementation of encryption is the protection of the content of a computer's hard disk. When the machine starts up the user must enter a password to access an encrypted partition on the hard drive. The information is then available for use. This method means that if the computer is stolen, the information on it cannot be retrieved. There are some potential problems – for example if the data on the disk is corrupted, in which case you might lose all of it. But as long as you keep a secure system of backups, disk encryption is a means of protecting information held on computers, and especially laptops (which are more vulnerable to theft).

The benefit of strong encryption systems is that you can put information beyond the reach of anyone who is not allowed to access it, and prevent digital signatures for emails or files from being altered and passed-off as the original. For those who work with sensitive information, or who need to securely transmit sensitive information over the 'Net, encryption and digital signatures represents a means of guaranteeing privacy and/or security.

The final strand in 'privacy technology' is the security of computer systems. Computers are a very efficient means of storing and manipulating information but they can become a security liability. An effort to protect privacy or confidentiality must begin with securing computer systems. A comprehensive beginners guide, *Introducing Information Security*, is available as part of the APC's *Participating With Safety* briefings[5].

Privacy law as a means of silencing criticism

On occasions, laws that protect citisen's privacy rights have been used to close controversial websites. For example, when the Association Against Torture in Spain published the names of those police officers and prison guards formally accused in Spanish courts of having tortured or mistreated prisoners, the ISP that hosted the site was threatened with thousands of euros in fines if it did not take the site down. Whilst opposedto what it interpreted as political censorship, the ISP was forced to comply for fear of being bankrupted by the fine.

Source: Asociación Contra la Tortura, http://www.nodo50.org/actortura/

4 See APC *Participating with Safety* briefing no.6, *Using the Internet Securely* – http://secdocs.net/manual/lp-sec/scb6.html

5 APC *Participating with Safety* briefing no.1, *Introducing Information Security* – http://secdocs.net/manual/lp-sec/scb1.html

Electronic Frontier Foundation Urges DoubleClick to Adopt Opt-In Privacy Protections

June 6, 2001

San Rafael, CA – Judge Lynn O'Malley Taylor ruled today that a lawsuit seeking to prevent DoubleClick from invading individuals' privacy moved one step closer to trial. The class-action claims in the privacy lawsuit against DoubleClick focus on DoubleClick's practice of tracking and profiling people without their consent as they browse the Web. She indicated that, unless the parties reach a settlement, the trial will be held in January 2002, despite DoubleClick's attempt to derail the lawsuit.

"DoubleClick is invading people's privacy by collecting personal information without first asking permission," said EFF staff attorney Deborah Pierce. "We are glad that Judge Taylor recognizes that DoubleClick's practices may be in violation of privacy rights guaranteed by the California state constitution."

"California's Constitution protects the general public against the massive, unauthorized accumulation of sensitive information," said Ira Rothken, lead plaintiff's attorney in the case. "DoubleClick's behavior is outrageous. DoubleClick's business model is flawed. And we are going to obtain a remedy from the court to stop them."

DoubleClick, an online advertising company, places banner ads and other website advertisements on behalf of its clients. The dispute concerns DoubleClick's use of cookies and web bugs to track the web browsing behavior of individuals. Individuals are often unaware these technologies exist, what they can do to avoid a cookie or a web bug, or how they can prevent companies like DoubleClick from placing cookies on their computer hard drives.

The lawsuit alleges that by using cookies DoubleClick can store personally identifying information, resulting in a profile of individuals based on their surfing history. Online profiling and aggregation of data from different sources allows others to form opinions, to market items, and to discriminate based on a profile that may or may not be accurate. Unwanted disclosure of information may have harmful consequences, ranging from simple embarrassment to serious problems such as harassment, violence, insurance cancellation, loss of job or home, and relationship issues with family and friends.

The Electronic Frontier Foundation (EFF), along with the Privacy Rights Clearinghouse (PRC) and the Electronic Privacy Information Center (EPIC), have been acting as advisors in the case, formally called *Judnick v. DoubleClick*.

Source: Electronic Frontier Foundation Media Release: http://www.eff.org/Legal/Cases/DoubleClick_cases/20010606_eff_doubleclick_pr.html

5 steps to better on-line privacy

1. Only conduct business, visit sites or become involved with web sites that have adequate privacy policies that cover:
   - To whom your information will be passed onto
   - Why the information is being collected
   - How the information will be used
   - Who will have access to it
   - How you can access the information
2. Install and use privacy enhancing software including:
   - Firewalls
   - Cookies
   - Web Bugs
   - Anonymous Web Browsing
   - Encrypted Email
   - Advertising Filters
   - Anti-Spam Tools
   - Further Information
3. Opt out of all further contact with the organisation when filling in on-line forms
4. Only give as much personal information as you are comfortable with
5. Use an on-line identity and free email service

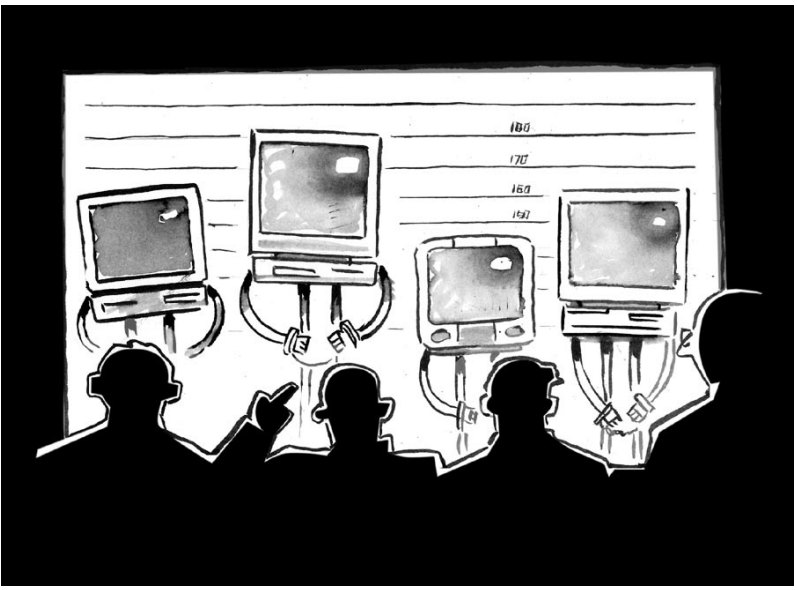
Source: "On-line Privacy Tools", Australian Privacy Commissioner, http://www.privacy.gov.au/internet/tools/index.html

22. Cybercrime and anti-terrorism legislation

Following the attacks on the World Trade Centre and The Pentagon on September 11th 2001, many states enacted laws to tackle the perceived threat of terrorism. At the same time, there was an increase in the dialogue and co-operation between the operators of the Internet and electronic networks, and the security services of many states. Although these measures were promoted as an essential part of the so-called 'war on terrorism', in fact many had been already in preparation before September 11th. The attacks merely led to faster implementation of technical and legal measures for the surveillance of individuals and organisations. September 11th also provided a perfect excuse to introduce measures that previously would have met more resistance from those concerned about how these new measures might erode essential civil liberties.

Most of these measures are aimed at tackling terrorism and serious crime, but at the same time many states have redefined the boundaries of these terms. There is a thin dividing line between everyday protest activities and what can be defined as 'organised crime'. This is typified by, for example, the UK's 'common purpose principle'. This new principle was created as part of the laws that gives investigative powers to police forces and the security services. It states:

"*conduct which constitutes one or more offences shall be regarded as serious crime where it involves conduct by a large number of persons in pursuit of a common purpose*"[1]



This principle has allowed the widespread surveillance of many protest groups in the UK. Whilst the offences these groups carry out are very minor (such as trespass and obstruction of the highway), the fact that they are carried out by many people working together allows them to be investigated with the same powers reserved for organised criminals.

When considering how the state has taken new powers to enable the surveillance of groups in society we must take note of this semantic re-definition. Terms such as 'cybercrime', 'terrorism' and 'organised crime' can be used under these new procedures to allow the surveillance of groups that oppose many aspects of government policy, as well as developments which may affect the economic well-being of large corporations. Organisations that may be affected by this redrafting of legislation, must consider these implications as part of their planning for future work and campaigns.

22.1. International legislative frameworks

The Cold War enabled the development of global networks of surveillance as part of military systems. Little information was thus publicly available about the functioning of these systems. In the post-Cold War era, these systems have been given legitimacy as 'security measures' to facilitate fight against international terrorism or criminal activity. Global surveillance systems that were developed out of the Cold War, such as the Echelon System[2] (a signals intelligence network developed the USA, UK, Canada, Australia and New Zealand), have pioneered new ideas for global surveillance networks.

1 *Police Act 1997*, http://www.legislation.hmso.gov.uk/acts/acts1997/1997050.htm, and *Security Services Act 1996*, http://www.legislation.hmso.gov.uk/acts/acts1996/1996035.htm

2 See *Interception Capabilities 2000* – http://www.cyber-rights.org/interception/stoa/interception_capabilities_2000.htm and http://www.echelonwatch.org/

In recent years, certain international bodies, such as the Council or Europe, the Organisation for Economic Co-operation and Development (OECD), or the G8 Conference, have begun to consider these issues as part of their policy agenda[3]. Whilst this has included extending co-operation on terrorism and security, an equally important strand in these discussions has been the development of policies on 'information systems'. The purpose of these policy discussions was to develop a common global standard for the retention of telecommunications and internet traffic data. For example, during the G8 conference in 1998 a set of principles, and a ten point action plan, were adopted, to 'preserve electronic data' for sharing between 'international partners'. This was followed-up in 2001 with a further conference workshop devoted to the preservation of data[4]. Initiatives such as this have in turn created an impetus for national legislation on the monitoring of electronic networks.

Within Europe, a significant development has been the adoption of the Cybercrime Convention[5] by the Council of Europe (CoE). The Council of Europe is an intergovernmental body formed from the 43 nations of Europe. Other states, such as the USA, also participate in the Council as observers. The CoE first proposed a convention to tackle cybercrime in 1995, which was finalised in September 2001. The Convention has three parts: the first proposes that all states criminalise certain on-line activities; the second that states require the operators of telecommunications networks or internet service providers to institute more detailed surveillance of network traffic, including where possible real-time analysis; and part three requires that states co-operate in the investigation of cybercrime by allowing data to be shared between them – even if the crime being investigated in one state is not a crime in the state from where information is requested.

As observers, the USA, Japan and Canada have co-signed the Convention. States in other regions are looking at the Cybercrime Convention as the basis for drawing up treaties on the sharing of communications data. Other states that are not members of the CoE are also free to sign-up to the Convention and co-operate with other states.

TreatyWatch: Eight Reasons the International Cybercrime Treaty Should be Rejected

"In November 2001, the members of the Council of Europe signed an extraordinarily broad new treaty to increase cooperation among law enforcement officials of different nations. Officially, this Cybercrime Convention was drafted by the 43-member Council of Europe, with the U.S., Canada, Japan and other countries participating as "observers." In reality, American law enforcement officials have been among the primary drivers behind the treaty.

The Cybercrime Convention does three major things:

1. It includes a list of crimes that each member country must have on its books. The treaty requires criminalization of offenses such as hacking, the production, sale or distribution of hacking tools, and child pornography, and an expansion of criminal liability for intellectual property violations (Articles 2-11).

2. It requires each participating nation to grant new powers of search and seizure to its law enforcement authorities, including the power to force an ISP (Internet Service Provider) to preserve a citizen's Internet usage records or other data, and the power to monitor a citizen's online activities in real time (Articles 16-22).

3. It requires law enforcement in every participating country to assist police from other participating countries by cooperating with "mutual assistance requests" from police in other participating nations "to the widest extent possible" (Articles 23-35).

This is a bad treaty, and nations should not sign or ratify it. There are 8 main problems with the agreement:

Reason #1: The treaty lacks privacy and civil liberties protections

Reason #2: The treaty is far too broad

Reason #3: The treaty lacks a "dual criminality" requirement for cooperation with the police of other nations

Reason #4: Protection for political activities is too weak

Reason #5: The treaty threatens to further unbalance intellectual property law

Reason #6: The treaty would give police invasive new surveillance powers

Reason #7: The treaty contains an overly broad criminalization of hacking tools

Reason #8: The treaty was drafted in a closed and secretive manner

Source: http://www.treatywatch.org/TreatyProblems.html (justifies these arguments)

3 *Policing high tech crime in the global context*, Dr. Paul Norman – http://www.bileta.ax.uk/99papers/morman.htm

4 See http://www.mofa.go.jp/policy/i_crime/high_tec/conf0105-5.html

5 Council of Europe Cybercrime Convention – http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=185&CM=1

What all these policies, such as the G8's action plan or the CoE's Cybercrime Convention, lack is a common definition of what is 'serious crime' or 'cybercrime'. There is also no requirement that before the data collected by a country is released it should be shown that the alleged actions would have been a crime if committed there. This means that there can exist wide differences in legal interpretation of the important terms, such as 'terrorism', 'serious crime' and 'cybercrime' between different states. This has significant implications for trans-national organisations that seek to challenge the actions of governments or corporations, particularly where these actions are primarily co-ordinated over the Internet.

22.2. The War on Terrorism

More than anything, the events of September 11th 2001 have led to an updating and expansion of 'terrorism' legislation to take it beyond the Cold War. Until recently 'terrorism' was defined as activities motivated by a political ideology for the overthrow of a government. The re-definition of terrorism by states since September 11th has stressed motivations other than political ideology, potentially classifying non-mainstream protest actions, campaigns and organisations as being involved in supportive of terrorism.

Terrorism, like cybercrime, is defined differently from state to state. In the USA, evidence given to the US Congress by the Federal Bureau of Investigations (FBI) stresses that any group that uses or threatens violence or damage against persons or property "*in furtherance of political or social objectives*" may be classified as 'terrorists'[6] . In the UK, the interpretation of new terrorism laws given by the government to local authorities stresses a much lower threshold, covering"*acts that may not in themselves be violent but which nonetheless but have a significant impact on modern life*"[7] . This supports the approach taken in the Terrorism Act 2000 (enacted a full year before the September 11th attacks) that redefines terrorism from some form of paramilitary action to any form of direct action or protest that "*seeks to change the mind of the government*"[8] .

The problem with these new laws is that they extend the definition of terrorism into areas of campaigning by civil society groups. Those engaging in mass protests, or taking direct action to disrupt trade conferences, the development of infrastructure projects, or the operation of private enterprises, risk being classified as 'terrorists'. In practical terms, these new laws will not allow the banning of most protest groups or the prosecution of their members as terrorists (although that could happen in the case of a few groups that take extreme action, such as *Earth First!*). However, those who associate or work with these groups can be investigated as if they were terrorists. In turn, the information gathered from such investigations could be used to restrict or nullify the actions of these groups.

Using Anti-terrorist Laws for other Objectives

"Citing a provision of the Patriot Act, the FBI is sending letters to journalists telling them to secretly prepare to turn over their notes, e-mails and sources to the bureau. Should we throw out the First Amendment to nail a hacker? ... The demand that journalists preserve their notes is being made under laws that require ISP's and other "providers of electronic communications services" to preserve, for example, e-mails stored on their service, pending a subpoena, under a statute modified by the USA-PATRIOT Act. The purpose of that law was to prevent the inadvertent destruction of ephemeral electronic records pending a subpoena. For example, you could tell an ISP that you were investigating a hacking case, and that they should preserve the audit logs while you ran to the local magistrate for a subpoena. It was never intended to apply to journalist's records."

Source: Mark Rasch, "The Subpoenas are Coming!",http://www.securityfocus.com/columnists/187

22.3. The implications for civil society groups

It is important to remember that most new terrorism legislation, and pretty much all the initiatives in relation to the investigation of serious crime/cybercrime, are based on the increased surveillance of communications. Groups that seriously challenge governments or multinational corporations could, under these legislative framework, come under direct surveillance. It is more likely though, that governments will use this new system to monitor and retain communications data in order to map the activities and the membership of campaign groups. This has implications for the functioning of these groups.

The late 1990s saw a surge in action by campaign groups coordinated via the internet. Electronic networking has facilitated the development of grassroots action at the national and international level. At the same time, this has left organisations that work in this way open to far more intrusive surveillance than other traditional groups. The membership of these organisations, even if they have no formal structure, can be mapped. The role of different members within the organisation can be analysed. From this data, opponents could devise actions against key individuals, or the network as a whole, to stop it from func-

6 See – http://www.fbi.gov/congress/congress01/freeh051001.htm

7 UK Home Office Circular 03/2001, *The Terrorism Act 2000* – http://www.homeoffice.gov.uk/circulars/2001/hoc0301.htm

8 Section 1, *Terrorism Act 2000* – http://www.hmso.gov.uk/acts/acts2000/20000011.htm

tioning. This is particularly problematic if the group is campaigning against the state, but would also affect anti-corporations campaigns. For those who engage in international action, there is also the problem that instruments such as the Cybercrime Convention would allow the supply of communications surveillance data from their home state, to another state, even if their actions were lawful in their home state.

There are two possible responses to the problems created by communications surveillance and the extension of anti-terrorism powers.

Those involved can practice good communication security. They can encrypt communications, use 'privacy enhancing technologies' (PETs) to restrict the disclosure of information whilst working on-line. They can also improve their own computer security to prevent the use of more active surveillance techniques such as the FBI's 'Magic Lantern' virus. The problem with this approach is that, at the public level, the organisation will take on the same pattern of activity as that practised by a terrorist group. This will make it easier for those who wish to restrict the activities of that group to take action, using the secrecy practised by the organisation as a justification.

The alternative to the good security option is the opposite in terms of tactics – not only does the organisation take no steps to restrict the disclosure of information via its communications, it actively seeks to be open. In addition, it uses every opportunity to enforce the rights of the organisation, or the individuals within that organisation, to have respect for the privacy of their communications, using legal opportunities to complain about the disclosure of information. An important part of this process is turning the network of mass surveillance into a campaign in itself. In this way, not only would it be difficult to characterise the organisation as a 'secretive' terrorist group, the organisation would be able to maintain an accessible public profile in order to build support for its work.

In practical terms, the solution for most organisations will be somewhere between these two options. Most of the time, being open is not a problem. But where the activities of the group involve working with those living under more repressive regimes, or where a group deals with sensitive information sources or whistle-blowers, the need to protect the identities of those individuals must be recognised.

23. Surveillance and data retention

Surveillance has been practised within society for millennia. Sun Tsu's text, *The Art of War*, written in the Fifth Century BC, contains details about surveillance and the 'use of spies'.[1] Over the past century the technology of surveillance has become increasingly more advanced, as have the means of avoiding and counteracting it.

There are two general types of surveillance: direct and indirect. The main difference between them is that direct surveillance can give you an idea of what a person or organisation is doing now, and by good analysis, what they intend to do in the future. Indirect surveillance only gives access to the past, via the information we generate every day, and so any inferences on what a person may be doing today or in the future are prone to error.

There are various forms of direct surveillance – such as telephone intercepts, bugging, and tracking the movements of people – each involving a different level of contact with the subject under surveillance. The more 'direct' the surveillance is, the more it costs.

Indirect surveillance usually involves no contact between the agent and the subject of surveillance. Instead it seeks to trace the evidence of activities. The use of electronic communications has aided the development of indirect surveillance. The retention of the data produced by communications systems has emerged as a new and powerful form of indirect surveillance. 'Dataveillance' – the use of personal information to monitor a person's activities – is a powerful means of monitoring the activities of an individual. What 'data retention' – the storage and use of information from communication systems – adds is the ability to map the interaction of groups of people as they communicate.

Computers have allowed the expansion of indirect surveillance because they can carry out a lot of work sifting information with minimal supervision. The impact of this process may also be to create so much information that the important facts are buried under a pile of other, less relevant information. The trade-off in the process of technological surveillance is that the information gathered is often not as good or as accurate as the old-fashioned human-based surveillance, carried out close to the subject. Often the information will be inaccurate, or out of the context in which it was gathered, and so may be interpreted wrongly.

There is very little that can be done to prevent surveillance – especially where it is carried out by the state. What can be done is to change your methods of working to make surveillance more difficult, or futile. This is called 'counter-surveillance', or in relation to computers and electronic communications, 'information security'. These procedures aim to minimise the disclosure of information to anyone monitoring your activities.

Counter-surveillance is the use of methods and technologies that create niches of privacy within our work. You should not seek to avoid surveillance for issues that have no sensitivity – to evade all surveillance may make you a greater target for surveillance as the state may consider your activities 'suspicious'. This of course assumes that sensitive work only constitutes a minor part of your work. If the sensitive parts of your work comprise a large part of your everyday workload, it would be more difficult to hide those activities within the patterns of your everyday life.

Information security aims to protect equipment with security procedures and barriers. When dealing with sensitive information, you should avoid generating any kind of documentation or opportunities that would facilitate surveillance. As governments begin to use communications and transactions data as a significant part of their effort to monitor the activities of their citizens, private communication is becoming harder to guarantee.

23.1. Methods of technical surveillance

Traditionally, the state has sought to intercept communications as a means of discovering the plans of individuals or groups. Although this process may be managed differently from state to state, in general there should be some form of judicial oversight or warrant to allow the interception of private communications. However, types of surveillance that do not involve intrusion into the privacy of communication do not always need judicial control. Controls over the intrusion into private communications have been further weakened as part of 'the war on terrorism', where the state may intrude into communications where under the guise of concerns about terrorist or criminal activity. The most significant of these is the use of communications data held by telecommunications companies or Internet service providers.

1 See Chapter XIII, *The Art of War*, by Sun Tzu. This can be found at many locations on the Internet if you conduct a search for the title and the author's name. Or try http://www.chinapage.com/sunzi-e.html

Telephone communications

For many working with information and communication technology, interception within the postal system is probably the least problematic. Almost every country that licenses postal or courier services including within the licensing process clauses on the interception of mail. The interception of telephone communications is more problematic. Intercepting mail requires the physical confiscation and opening of the mail, whereas a telephone intercept only requires that the line be tapped at the telephone exchange, and the information from that tap routed on another phone line to the surveillance operative.

The interception of telephone traffic has become more sophisticated in recent years. Forty years ago each telephone tap had to be monitored by an operative placed at each telephone exchange the call was routed through. Today, because all major exchanges are digital, the telephone traffic can be monitored by a computer. Instead of requiring manual connections, telephone taps can be set up changing the route your telephone calls take. The call can then be copied, and the copy routed to the agency that monitors phone calls for the state. Other features, such as 'caller ID' (where the number of the person calling is sent down the line and displayed), make it easier for the source of telephone calls to be discovered instantly.

The ability of digital exchanges to produce itemised bills for customers is also an indication of the level of information that can be produced for surveillance operatives. In many states, the use of this 'communications information', rather than the content of the telephone call itself, is not controlled under the same stringent legal procedures. This means that surveillance agencies are able to use billing data from phone companies, and any other organisation that keeps itemised information about your life, with far less controls than if they used direct tapping of your communications. Although this information does not contain the content of a particular action or communication, by merging information from a number of people's billing records it is possible to determine relationships and habits between individuals that can disclose equally valuable information.

The media image of phone tapping is that of a surveillance operative with a bank of reel-to-reel tape recorders. These, like the telephone systems, have been replaced by digital systems. The latest telephone surveillance systems sort the faxes from the telephone calls from the computer data (and store the faxes/computer data for later investigation). They also listen for keywords within the telephone conversation, or the presence of a certain person's voice on the line, and flag that particular call for analysis by a human operative. This increases the number of telephone taps that may be run by a single surveillance operative, making it easier to tap more lines.

The internet

The interception of Internet traffic is technically more problematic. Unless the interception can be fixed at the point where the person accesses the internet (their phone line or network connection), it is not possible to gather the information sent or received by one individual. This is because the communication is split into small 'packets' of data, and these may be routed by different communications channels. For this reason monitoring the Internet has preoccupied a number of states for the last decade. Their answer is, in short, to monitor everything and compile the 'communications data' gathered from this process for later use.

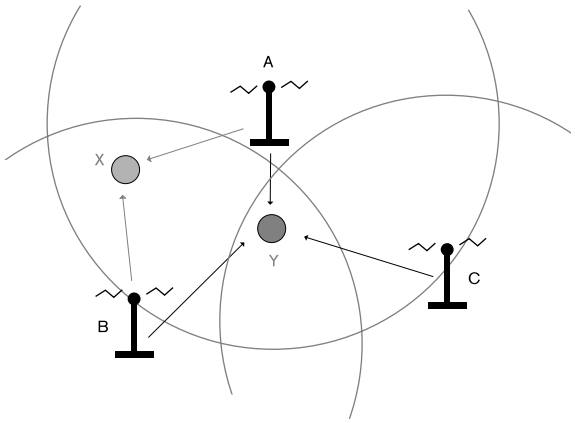
Tracing 'Net usage involves the lowest level of Internet identification – IP addresses. Most internet systems, such as email servers, log additional data. Most email servers log the 'header' information of the emails they relay. At a minimum, which address the email has come from, which address it is going to, and the date and time. This provides an even shorter route to finding the source, as an email address can be associated with a user account directly. From the service provider's records, this then translates to a real identity. This identity may be uncovered simply by searching on-line for the user's real name. Even if the source address of the email is forged or 'spoofed', the email server will still log the IP address of the machine it was sent from – so it can still be tracked back.

Mobile phones

It is also possible to track people's physical location using wireless communication devices such as mobile

phones or wireless computer networks. Mobile phones stay in constant communication (unless switched off) with their network's nearest base station. Knowing the location of this base station gives a rough geographical location. But it is also possible for the telephone system operator to gather data from other base stations to track the phone's position.

As well as recording which base station the phone is near to, most phone systems record a 'signal to noise ratio' (SNR) – a measure of how strong the signal from the phone is – for the signal to adjacent base stations. By getting the SNR from base stations near to the phone (which can be done in near real time with the co-operation of the telephone operator) it is possible to estimate the position of the phone between the stations quite accurately. The more base stations there are, and the closer together they are, the more accurately the position of the phone can be determined. In rural areas base stations may be 5km or 10km apart. In urban areas, separation may only be a few kilometres, and much less in built-up cities. This means that a person's position can easily be determined to within a few tens of metres in an urban area, or slightly more in a rural area.



The new 'Third Generation' (3G) mobile phones have a smaller separation distance between base stations. It is also proposed that 3G phones will use tracking routinely as part of the operation of the system. Not only to find a person's location, but also to identify the location of phone numbers (public services, advertising information, etc.) for users. This will mean that more information about a person's location at a specific date and time will be routinely generated and passed on to others. How states handle the security and privacy of this information will determine whether the 3G mobile phone will become a liability to personal privacy over the next few years. If communications and privacy regulators seek to protect this information as they do with other personal data, only official uses of this information will be possible. But if the data is poorly controlled, the collection or disclosure of this information could be used as a means of invading private life. It could also leave a person open to various types of fraud or crime because those directing the individual will know where the person is located.

In the future, as access from devices such as digital telephones and TVs, or 3G mobile phones becomes more widespread, accounts will be authenticated as belonging to a single person who owns that device. This trend for user authentication is at the forefront of many IT developments because it will enable the greater use of payper-use or subscription services on-line. It is enabled by systems such as Microsoft's '.Net' ('dot-Net') standard, which aim to build secure user authentication into networked systems. This uses a unique on-line 'passport', held by a verification server, to verify the identity of the individual as part of on-line transactions. But at the same time, it provides traceability, and a consequent reduction in anonymity, in a way similar to the way credit card transactions can be easily traced to a particular card holder.

Computers

Computers, and information systems in general, present various opportunities for surveillance. This is because they are technical systems that operate largely beyond the understanding of their user. An emerging new field is 'spyware' – computer software that is intended to collect information about a person's use of information systems. In addition, companies that specialise in 'computer security' systems are producing software applications that are able to interrogate a computer and retrieve information, passwords, and even deleted files.

Many computer systems routinely log information when they are used. Other programs, such as web browsers or word processors, log information relating to the use of the program, the files looked at, and the identity of those accessing or modifying files. These logs can be extracted if someone has access to the computer, and are a critical source of information in the field of 'computer forensics'.

The development of computer software that is specifically intended to spy on computer users represents a serious risk to privacy. Even where logging facilities do not exist on a computer, logging programs can be installed to monitor specific uses of the computer. These can collect information on the keys that are typed by the user, or the email or Internet addresses that are contacted. The program then stores the information for later retrieval, or the information could be emailed out covertly when users check their email. An example of this type of software is the US Federal Bureau of Investigations (FBI) 'Magic Lantern' program[2]. This was designed to find its way into

2 *FBI Confirms 'Magic Lantern' Project Exists*, Reuters, 12th December 2001.

certain computer systems and send back details about the content of the computer, account passwords and encryption keys. Controversy was aroused when the FBI attempted to conclude an agreement with anti-virus system writers to make sure their virus programs ignored the Magic Lantern program when it had installed itself on someone's computer.

One routine means of collecting information as part of the surveillance process is collecting people's rubbish. Important information is routinely thrown away by many people. For users of information systems, what is thrown away may also disclose information about security procedures, and even large quantities of sensitive data. For example, throwing away old floppy disks, CDs, even if they do not appear to work, can disclose important information to those with the ability to read corrupted or damaged storage media.

23.2. Dataveillance

Whilst people may fear high-tech electronic surveillance, often what betrays information the most is human nature: mistakes, forgetfulness, or unintended disclosure. Indirect surveillance techniques, which study the information we generate as part of our everyday activities, are good at picking these up.

The significant process within indirect surveillance is the finding of audit trails or documentation trails. Before the

widespread use of data processing this was a cumbersome business as paper had to be shuffled. Today, with so much information being digitised, and even sold in bulk by governments and corporations, the process has become far simpler. For this reason, indirect surveillance that concentrates on the use of digital information has become known as 'dataveillance'.

To organise any information you must have an index or 'key'. The key which everyone possesses is their name. But this key is not unique. Other people within a large town, and almost certainly within a country, will share that name. For this reason it is necessary to qualify the 'name' key with other identifiers, for example, an address, national identity or social security number, or credit card number. By increasing the number of additional key values that we group together we increase the likelihood that the surveillance subject, and only the surveillance subject, will be identified.

The state, via its security organisations or the police, is able to officially access large quantities of digital information. This can be done via state agencies, such as tax or social security agencies, or by the use of legal powers to obtain information from organisations that hold data about you, such as phone companies or banks. Depending on the nature of the 'offence' that you are being investigated for, the police and other agencies may also have access to legal powers to intercept direct communications and even enter a building to obtain additional information to enhance their analysis.

What this process produces is a 'data profile' – a set of information that relates to a person and describes his/her life, work, acquaintances, personal preferences and personal habits. More usefully, by merging information or 'data matching', using the information on more than one subject, it is possible to 'map' the interaction of a number of people. This may disclose further useful information, such as how an organisation relates to its supporters. Combining information that gives geographic data, such as the locations of purchases, or mobile phone tracking data, it is also possible to show patterns of collective activity, such as meetings, or travel to a particular location.

23.3. Managing the impacts of surveillance

For information-based surveillance techniques to work well there are certain pre-requisites:

- Information must be logged and stored, or routed in such as way as to make it available to those carrying out surveillance.
- Any encryption or technical encoding/compression must be susceptible to circumvention by those carrying out surveillance.
- Information must be identifiable with a unique, personalised key, or machine addresses, so the information may be tracked back to the people involved.
- For reliability, the surveillance process must work within the operation framework of the system supporting it so that it cannot be avoided or circumvented by the user.

When evaluating the surveillance potential of legislative proposals, or of technological innovations, we can use these three conditions as a guide. Conversely, any system that achieves the opposite of these conditions will lessen the impacts of surveillance.

For example, the greatest damage to civil liberties would be the 'cashless society', where every transaction had to be paid for with a credit or debit card. This is because cash, except for the larger value bank notes, is an anonymous form of payment. But in the cashless society, every payment made would be open to scrutiny. Likewise, if everyone across the globe would have a unique on-line identity that, like a passport or bank account, required verification before use, all anonymity on the 'Net would be lost. What enables privacy and anonymity generally on the Internet is that a person need not prove their identity in order to gain access to the network. They need only produce a user name and password that satisfies access to a particular user account.

These examples may seem extreme, but in the virtual world there are already well-advanced projects to implement such systems on-line. The next generation of Microsoft operating systems will begin to implement 'trusted computing platform' controls. These protect intellectual property rights by monitoring the status of information on a system, and what is being done to it. However, the unique identifiers that will have to be applied to all files, based upon the registration of the software that generated them, will mean that information may be easily traced to its source.[3] Also, the development of on-line e-commerce systems around the 'dot Net' model, where people use an on-line identity to verify access to sites or for payments (in place of a credit card number or password), means that the ability to track activity on-line will be enhanced.

The extension of intellectual property controls generally has a negative impact on privacy and security. It is more difficult to verify that the programs you use do not contain unknown data logging systems or 'back doors' that give access to password protected or encrypted data. If someone attempts to reverse-engineer the program in order to reveal such flaws, they could be prosecuted for damage to the developer's intellectual property.

There are many applications in use on the 'Net today that contain some form of user monitoring and reporting facility[4]. Some of these involve the use of the program ' spyware'. Others are used as a means of targeting the user with adverts – 'adware'. Program developers include these systems, particularly adware features, as a means of obtaining extra revenue from the use of their applications. Many widely used programs, such as Real Player, AOL Instant Messaging and Kazaa, contain these systems.

Unless you install the program on your system, most of these spyware and adware programs use the 'cookies' facility in the web browser to store data on your computer, to enable tracking of your activities on-line. 'Cookies' enable a web site to store information about your use or preferences on the site so that the server can personalise your access to the site when you next return. But they also allow tracking of an individual's on-line activity, and thus can be used as a unique identifier available to web advertising agencies and others to follow you on-line. For this reason they are being restricted and controlled informally (the W3C Consortium's 'Platform for Privacy Preferences' system), or formally (the recent proposals by the European Union to legislate against the use of cookies).

---

3 http://www.asp.net, http://www.passport.net/, http://alive.znep.com/~marcs/passport/

4 There are good reports on spyware/adware available online from ZDNet (http://www.zdnet.com/zdnn/stories/news/0,4586,2678941,00.html) and fromBBC Online (http://news.bbc.co.uk/1/hi/in_depth/sci_tech/2000/dot_life/2487651.stm) also:http://www.cexx.org/adware.htm, http://www.doxdesk.com/parasite/

The alternative is of course, where possible, to use free software on computer systems. The fact that the computer source code is open means that it is far harder to hide 'spyware' within the code of a computer program. Those concerned with the impact of surveillance on their use of information systems should seek to change their patterns of use to make surveillance more difficult[5]. However, increasingly the 'intelligent appliances' that we use, such as mobile phone or personal organisers, have their software sealed inside. So using open source alternatives to proprietary systems can only work up to a point. But wise use of these appliances, such as consciously switching off your mobile phone before going to sensitive meetings, can minimise the surveillance potential of these devices.

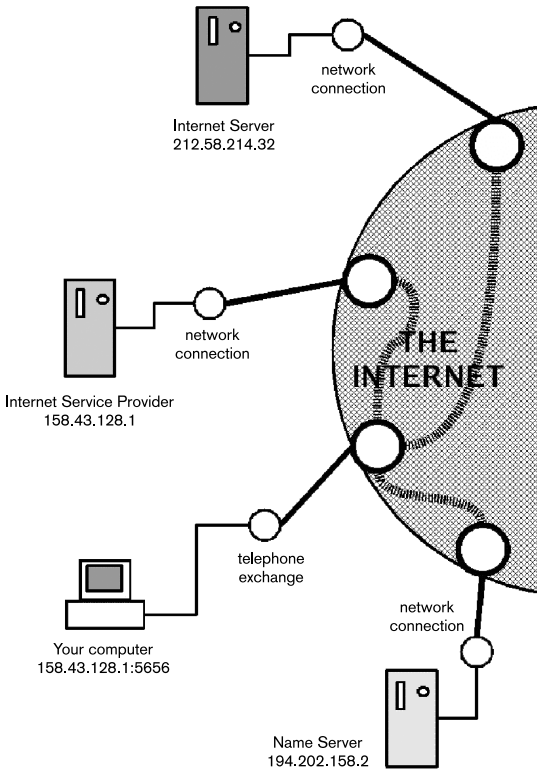
23.4. Data Retention

Electronic networks, be they the wires that make up national telephone networks, or the network of networks that is called the 'internet', are becoming the main means by which society works. Over the last 10 years various governments around the globe have taken the view that ability to monitor, and perhaps police the use of electronic networks is a key part of keeping order within the new information society. The problem with monitoring networks is the volume of data involved.

It is not possible to just jack-in to the network and monitor everything that is sent. Or rather, it is technically possible, but not physically, practically or economically viable. For this reason, states are addressing the problem by seeking to ensure that certain types of **communications data** be 'retained' by the providers of network services. This data can then be accessed by the state.

Tracking access

To begin, we need to understand a little about the workings of the network itself. When you make a phone call, you dial the number of the receiving station, and you are connected. This is because your number, and the number you are calling, are unique, and can be easily identified by the equipment that makes the network function. A route is then set up between these two points for the communication to flow along. The internet applies this same principle, albeit with a little more complexity. The diagram on the right shows a number of computers linked to the internet. The internet has no fixed structure. Packets of data can be routed randomly. For this reason we can only show it as an amorphous mass to which computers connect at specific nodes.



Most individuals and small organisations connect to the 'Net via a 'network connectivity provider'. This could be your local telephone company, your place of work, or a private Internet service provider. This provides you with access to the network via a local phone number. It also, although most people do not realise it, connects you via the local telephone exchange to the internet as part of the 'domain' of your service provider. Like your own name and telephone number, this provides you with a unique identity on the internet. Not everyone can have a address – there are not enough to go around. Instead you will be allocated a number on the machine that logs you onto the Internet. This machine then relays the information between you and the internet.

Now that your computer has the IP number of the service you require, you make direct contact to that server via the Internet. Nearly all internet services – web, email, chat, file transfer – log the IP address of the communications they receive. This means that if someone can access the log data for a particular server, they are able to create a list of who accessed that server and when. The first stage of finding who accessed that server is to track back the IP address of the packet. This will take them to the server that logged you onto the internet. This may be your service provider's server, or it may be another server that

5 For a more detailed briefings on counter-surveillance and information security see the Association for Progressive Communications *Participating with Safety* briefings at http://secdocs.net/manual/Ip-sec/These outline the improvements that can be made to computers and working practices to improve security and reduce the effectiveness of surveillance.

your service provider uses to provide local network access. Either way, there will be a log there that indicates the identity of the user account that logged onto the network with that IP address at that time. Using the local network identity, or the user account identity, it is then possible to match a user's real name to their login account. If this account was at a cybercafé or university, if someone paid for the session using some sort of credit or debit card, it may also be possible to trace the person from the payment details attached to that period of usage. For further confirmation, the billing information kept by the phone company will also confirm that at that time and date that a person used the phone to connect to the Internet.

Even before the September 11th terrorist attacks, many states were drafting or introducing laws that enabled technological surveillance to take place within new digital information systems. For example, in the USA the Communications and Law Enforcement Act 1995 requires that manufacturers of telecommunications equipment get approval, to ensure they comply with tapping or surveillance requirements, before a new product is sold. Many of these new laws relate to the information or 'communications data' that digital systems generate. It is claimed that these systems do not represent the development of a 'Big Brother' state because access was not being granted to the content of communications. This misrepresents the impact of these new surveillance systems. The automated nature of these systems means that far more people can be monitored than was previously possible with human-based systems.

Mandating data retention

Most communications network operators would not wish to keep large quantities of data about the operation of their systems. In some countries, such as European Union states, it creates legal liabilities because of data protection laws. In general, keeping this information is a time consuming, resource hungry and costly operation. For this reasons some states are now legislating to make data retention a legal obligation of the operators of electronic networks.

Keeping logs on a server costs money. It uses up some of the server's processing capacity and disk space. If the logs have to be kept for a period of time, it will also be necessary to back-up these logs to some sort of storage media and store them securely for that period. To date, one of the principal obstacles to implementing the retention of log data has not been civil liberties, but cost. Internet service providers have been concerned that proposals to monitor network traffic would place high costs upon their businesses.

The other problem for governments has been how to handle this data. The traffic data produced by the telephone system is huge, including millions of numbers, each logging many outgoing calls every day. This may be dwarfed by the potential data harvest from electronic networks, including logs from internet service providers, email servers, web servers, and other sources such as the log information provided via the data retention systems of other states. For example, the Cybercrime Convention defines 'traffic data' as:

- a code indicating a network, equipment or individual number or account, or similar identifying designator, transmitted to or from any designated point in the chain of communication;
- information on the time, date, size, and duration of a communication;
- in any mode of transmission (including but not limited to mobile transmissions), any information indicating the physical location to or from which a communication is transmitted.

On top of this, other data streams are likely to be added. For example, in the USA, it is proposed that the 'Total Information Awareness' (TIA) programme (recently renamed the 'Terrorist Information Awareness' programme) will add data from sources such as public lending libraries, credit card transactions, ATM withdrawals or even seat reservations on aircraft in order to try and link geographical references to communications traffic.

The problem is that none of this data can be isolated to concentrate on a few individuals. Unless the state instructs a service provider to specifically tap the connection of a particular person, the data retained by a server operator must be collected for all users. That is a lot of data to store. The fact that people other than the principal targets of surveillance are included increases the probability that their privacy may be damaged as part of the retention and processing of communications data.

The UK was one of the first countries in the world to require the widespread monitoring of all network traffic. In the UK, the retention of log data by the government was under discussion in the mid-1990s. Initially, discussion within the police and security services assumed that it would be possible to limit monitoring to a few individuals. But when that was clearly not possible, the proposals were soon expanded to allow for the tapping of *all* network traffic. This was originally conceived as a 'black box' working inside every internet service provider's machine. The proposals were later modified, taking advantage of the fact that most service providers are connected directly to one of the large telecommunications networks. For this reason, the proposals now target 'upstream providers', and the larger internet services, in order to reduce the number of locations that will have to log all traffic data.

The law that required the disclosure of traffic data in the UK, *The Regulation of Investigatory Powers* (RIP) *Act 2000*, was enacted almost a year before the attack on the Twin Towers and the launch of the 'war on terrorism'. However, there were some gaps in this law. It required logs to be turned over, but did not explicitly require that they be kept. For this reason the proposals were updated in *The Anti-Terrorism, Crime and Security Act 2001*. In addition to requiring the operators of electronic networks to set up 'interception capabilities' on request, the RIP Act also sets up a 'technical advisory body' to advise the government. Its job is to assess the current technical capabilities for the collection of data, and the interception of communications, and to look for means to implement these as part of interception requests that government may issue to individual network operators. But recent difficulties have made its future uncertain.

Due to its pioneering steps in trying to develop data retention nationally, the UK has been one of the lead states in developing international systems for data retention[6]. The key agreement to date has been the Council of Europe's *Cybercrime Convention*[7]. The Cybercrime Convention requires that states take measures to preserve the data produced by electronic systems, such as telephone networks and the internet. States can then make requests to other signatories of the Cybercrime Convention to access data relating to the activities of certain individuals or groups resident in that state.

Other states are also seeking to develop their own systems to intercept and process communications information, as well as information from other sources. Perhaps the most high-profile of these at the moment is the proposal for a 'Total Information Awareness' (TIA) system in the USA[8]. The original proposal in the USA, at the end of the 1990s, was a smaller system called 'Carnivore'[9]. This would have monitored the communications of certain 'suspect' individuals, groups or web sites. There was much debate over the legitimacy and legality of the Carnivore system. Following the September 11th 2001 attacks, the legal basis for mass surveillance has changed – hence the reason why the TIA system is able to do much more.

In many states in the developed world[10], after the September 11th attacks new legislation that broadened the surveillance powers of the state was introduced, using the attacks to silence dissent about the impact of these powers. These kinds of sweeping surveillance systems are not perfect, and This means that errors in the analysis provided by these systems are likely to crop up on a regular basis, leading to the potential for serious miscarriages of justice to take place.

What these new powers have introduced is a means whereby the state is able to conduct detailed indirect surveillance of the entire population. The problem is that the systems that enable this, and more importantly the information they relay on, are imperfect. Errors in the analysis of the data provided by these systems can lead to serious miscarriages of justice.

Carnivore campaigns

The first anti-Carnivore campaigns simply called for email users to include key words, such as terrorist, bomb, explosive, White House, etc, in their emails, so as to confuse and clog up the classifying programs used in the Carnivore project. Later they became more explicitly political and attempted to influence the US government:

"If we want to defeat Carnivore, we need to attack on all fronts. Any of the following steps could take you as little as one minute each to complete, and they will all make a big difference in the strength of our message. If you are able, spend a little extra time writing some comments of your own to send out to the various people below. If not, use our ready-made letters, and make a big difference in under 10 minutes!

1. Tell a friend about this site
2. Contact the President and Congress
3. Send a Letter to the Editor
4. Contact John Ashcroft
5. Check Your ISP

Source: http://stopcarnivore.org/how_to_stop_carnivore.htm

Problems with data retention

There are many ways in which data can be collected from diverse sources, and then used to create data profiles. This process is also described as 'data matching', because it requires the sources of information to be matched

6 For a recent review of the UK's influence on European developments see *UK Pushes Boundaries of Citizen Surveillance*, The Guardian, 12th June 2002 – http://www.guardian.co.uk/netprivacy/article/0,2763,736011,00.html

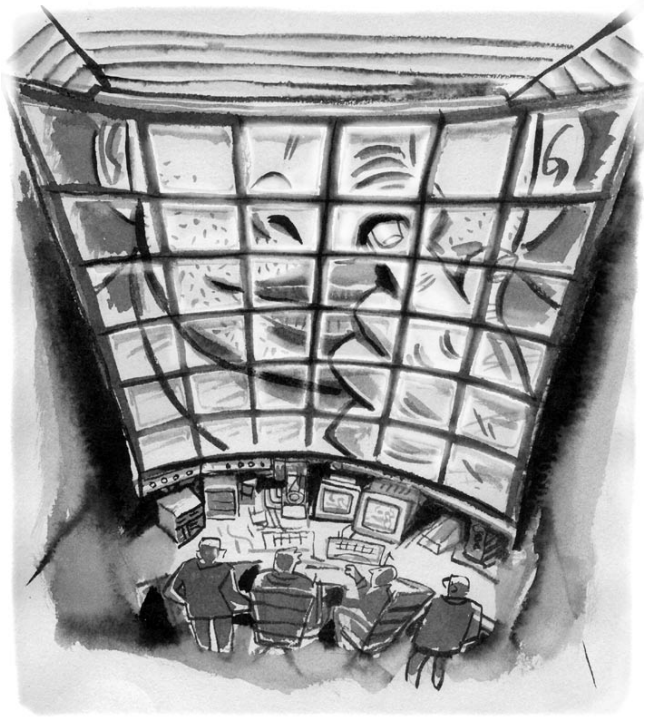
7 See http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=185&CM=1

8 See the archive kept by the Electronic Frontier Foundation for a digest of available information on TIA systems - http://www.eff.org/Privacy/TIA/

9 The FBI revealed its work on the Carnivore programme in a presentation to Congress in April 2002 – see http://www.house.gov/judiciary/corn0406.htm

10 For example, see UK Pushed Boundaries of Citizen Surveillance (Guardian, June 12th 2002). For other more detailed reports go to the *Electronic Privacy Information Centre*, http://www.epic.org/, and *Privacy International*, http://www.privacyinternational.org/

around a common set of indexes or 'keys'. This has the potential to create spurious results from matching different data sources that may lead to serious breaches of civil liberties.



One of the basic assumptions regarding electronic networks is that they are synchronised, and all log transaction data use a common date and time. This is often not the case. In the USA recently, as computer data has become an important investigative tool, there have been some miscarriages of justice due to inconsistencies in log data. In one case three young women were wrongly arrested and charged with murder, and spent three weeks in custody[11]. The evidence for the charge was that they had been photographed on an ATM machine's video camera using the cash card of the murder victim.

Time is becoming an increasingly problematic issue within the operation of global electronic networks. Whilst there is a general 'Universal Time Constant' in use, there is no international agreement on the precise setting of the clocks that control the global electronic networks. The networks operated by different countries, or by different corporations, may be set to slightly different times. The greatest problem is that many electronic systems do not use one central time reference. They have to be manually updated, and this, due to the human element, does not reliably take place. This in turn results in the sort of error that occurred with the ATM video evidence in the murder investigation described above.

Another problem with collecting traffic data is that the same types of data may not be collected consistently. Errors may be introduced due to inconsistencies in the classifications of certain goods or services, or because of language differences. This can lead to the inclusion of erroneous information as part of data profiles.

Further problems may arise due to errors in the data matching software that excludes some information, or wrongly includes it. As the logging of data is not considered to be a 'mission critical' part of the operation of electronic networks, the logging of data may be subject to errors that do not show up in other parts of the system's operation. In order to take into account the differences in data collection standards the systems developed for data matching may build-in some flexibility in their interpretation of data. This in turn may increase the likelihood that false positives will be produced as part of the process.

Perhaps the greatest challenge to the use of the data collected from monitoring networks is identity theft. At the basic level, an identity could be forged, or a user account or telephone line hacked into, in order to use the service without disclosing the true identity of the user. At a more complex level, if people can obtain sufficient information about an individual, they may be able to steal that person's electronic identity outright. This practice is already widespread as part of credit card fraud. As networked systems increasingly use individual electronic identities, rather than a user account, to validate access, identity theft may create a new level of abuse. Rather than just defrauding banks and credit card companies, identity theft in the future may be a means of avoiding the interlinked web of monitored networks that data retention is creating.

The problems of false identities, or identity theft, have significant implications for the effectiveness of new surveillance systems. In particular, they strike at the heart of the justification for developing these systems. The groups with the capacity to undertake identity theft are organised criminals and terrorists – precisely the groups these systems are meant to detect. So, in practice, these systems are only fully effective against one particular group in society – the general public.

If we look a few years ahead, when networking becomes more personalised, tampering with a person's identity may become a major hazard to personal privacy and civil liberties. Locational data from wireless device, if poorly protected, could be used to target individuals for crime and aid in the execution of a crime, as well as undertake fraud or identity theft in a way that is far harder to trace. The problem with the systems being deployed today is that

11 See http://www.washingtonpost.com/wp-dyn/articles/A19633-2003Jun21.html

they are keyed to record data about an individual, or an individual's access, thereby making fraud or identity theft easier to operate. The alternative, using anonymous systems of authentication, is not welcomed by financial institutions and governments because they do not allow the tracking or auditing of an individual person's activity from the log of communications data. Anonymous systems of authentication – for example use-once credit card numbers issued by some card companies for use on-line – would make it far harder to obtain sufficient personal identifiers to impersonate or abuse electronic identities on-line.

Reasons why we should oppose dataveillance (summary)

1. People collect, or process information for a purpose. It is the intention of those who collect personal information, or who trade or database it, to create profiles of individuals. Individual users may not necessarily give consent to the use of their personal information for that purpose.
2. The sale of personal information is, for many Internet companies, a major income stream within the operation of Internet services.
3. The suppression of encryption may mean that those who break the law will encrypt anyway.
4. Information gathered in the process of technological surveillance is often not as good or as accurate as the old-fashioned human-based surveillance, carried out close to the subject. Often the information will be inaccurate, or out of the context in which it was gathered, and so may be interpreted wrongly.
5. Types of surveillance that do not involve intrusion into the privacy of communication do not always need judicial control
6. If the data is poorly controlled, the collection or disclosure of this information could be used as a means of invading a person's private life. It could also leave a person open to various types of fraud or crime because those directing the individual will know where the person is, or is not located.
7. 'Cookies' allow tracking of an individual's on-line activity, and so are useful as a unique identifier available to web advertising agencies and others to follow you online.
8. The fact that other people than the principle targets of surveillance are being included increases the probability that their privacy may be damaged as part of the retention and processing of communications data.
9. Problems with the accuracy of data collected:
   - Data collected from different sources has the potential to create spurious results from the matching process, which may lead to serious breaches of civil liberties if the results are acted upon by law enforcement agencies.
   - The same types of data may not be collected consistently, which can lead to the inclusion of erroneous information as part of data profiles.
   - The networks operated by different countries, or by different corporations, may be set to slightly different times, which may lead to erroneous conclusions about persons' whereabouts at a certain time.
   - Another problem with collecting traffic data is that errors may be introduced due to inconsistencies in the classifications of certain goods or services, or because of errors introduced by language differences. This can lead to the inclusion of erroneous information as part of data profiles.
10. Perhaps the greatest challenge to the use of the data collected from monitoring networks is identity theft. Rather than just defrauding banks and credit card companies, identity theft in the future may be a means of avoiding the interlinked web of monitored networks that data retention is creating.
11. The groups who have the capability to routinely undertake identity theft are organised criminals and terrorists – precisely the groups who these systems are meant to detect. So, in practice, these systems are only fully effective against one particular group in society – the general public.

24. Visions of the Right to Communicate

The notion of human rights is based on the understanding that everyone in society should be free to participate fully in social and political activities and to be protected from attempts to restrict the exercise of this right to citizenship. In various countries it has been extended further, to include cultural and socio-economic rights (such as the right to health care, housing and clean environment), also known as second and third generation rights. Whether we can simply extend the existing set of rights to apply to the realm of the 'information society', or need rather to formulate a new set of rights such as communication rights, digital rights, and internet rights – and what would be the content of these rights – are issues addressed in this chapter.

Towards a perspective on the Right to Communicate

Different rationales have been expressed to support formulation of a new or emerging right to communicate. In a broad sense, its advocates appear to act out of a concern that increasingly, the media are becoming homogenized and minority or dissenting voices are rarely heard.

Globalisation and commercialization of the media is one of the chief concerns: it is argued that in countries around the world, threats from the private sector–such as large media corporations–are as harmful to the right to freedom of expression as traditional state threats. Whilst in many African countries, it is the state which is the problem by imposing restrictive rules and regulations on freedom of expression or by itself dominating the media sector while failing to reflect the diversity that exists within its territory.

The formulation at the international level of a right to communicate, it is said, would remedy both of these problems. Legal recognition of a right to communicate would additionally help bridge the growing digital divide by empowering those currently left behind in the communications revolution.

However, there appears to be little agreement on the precise definition or content of the right to communicate. How is it different from the right to freedom of expression or to what extent such a right or a Declaration would fit in the existing international Bill of Rights (formed by the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights)?

Source: J Barker and P Noorlender, *FreePress magazine* (April 2003) of the Media Institute of Southern Africa, also available at: http://www.dgroups.org/groups/IS/index.cfm?op=dsp_resource_details&resource_id=3169&cat_id=2779

Human Rights have been codified in a large number of UN declarations, covenants, treaties and agreements. The clearest and most important expression is the Universal Declaration of Human Rights, agreed to by the UN General Assembly in 1948. This was followed in 1966 by the International Covenant on Social, Economic and Cultural Rights, and the International Covenant on Civil and Political Rights. Subsequent resolutions by the General Assembly or UNESCO have addressed specifically the human rights of women, children, and indigenous peoples, for example, with reference to issues of cultural diversity, science and technology, language, and development, among others. Of particular relevance in out context is the way in which the various UN agreements on human rights refer to science and technology, as discussed by Cees Hamelink in a number of articles.[1]

Hamelink has called for the specific consideration of communication rights, which are not covered by existing agreements. In his view, communication should be understood as an interactive process, in essence "a process of sharing, making common or creating a community".[2] We do not need 'information societies' – implying a flow of information in one direction – but rather 'communication societies'. Hamelink sees the recognition of a right to communicate as 'essential "if global governance of 'communication societies' should be inspired by human rights concerns."[3] In attempting to specify the content of the

1 C Hamelink, "The Right to Communicate", paper presented at Prepcomm1, (2002), http://www.geneva2003.org/home/events/documents/gen_hamelink_en.htm, and "Human Rights for the Information Society", Briefing Paper Series for the WSIS (UNRISD), 2003

2 Hamelink, 2003.

3 *op cit.*

UN Agreements referring to human rights and science and technology

Universal Declaration on Human Rights (1948)

The Universal Declaration of Human Rights (1948)

The Convention on the Prevention and Punishment of the Crime of Genocide (1948)

The Third Geneva Convention relative to the treatment of prisoners of war (1949)

The UNESCO Hague Convention for the Protection of Cultural Property in the Event of Armed Conflict (1954).

The International Covenant on Civil and Political Rights (1966)

The International Covenant on Social, Economic and Cultural Rights (1966)

The UNESCO Declaration of the Principles of International Cultural Co-operation (1966)

The Declaration on Social Progress and Development (UNGA, 11 December 1969)

The UNESCO Convention on the Means of Prohibiting and Preventing the Illicit Import, Export and Transfer of Ownership of Cultural Property (1970)

The UNESCO Convention for the Protection of the World Cultural and Natural Heritage (1972)

The Declaration on the Use of Scientific and Technological Progress in the Interests of Peace and for the Benefit of Mankind (UNGA res. 3384, 1975)

The UNESCO Recommendation 'Participation by the People at Large in Cultural Life and Their Contribution to It' (1976)

The ILO Declaration on Principles Concerning Multinational Enterprises and Social Policy (1977)

The Convention on the Elimination of All Forms of Discrimination against Women (1979)

The UN Declaration on the Right to Development (1986)

The Convention on the Rights of the Child (1989)

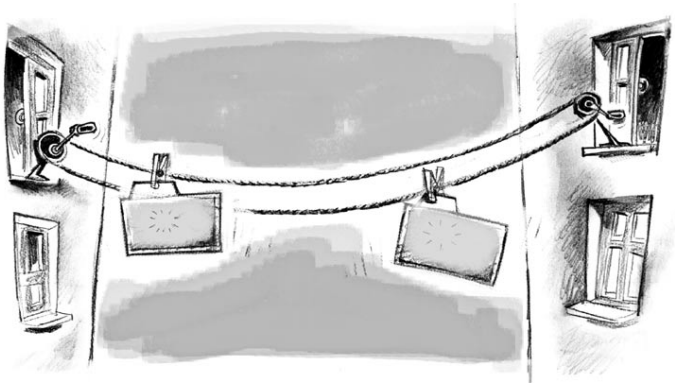
The 1989 UNESCO Convention on Technical and Vocational Education

The UN Draft Declaration on the Rights of Indigenous Peoples (1994)

The UNESCO Universal Declaration on Cultural Diversity (2001)

Source: Hamelink (2003)

right to communicate, he lists a large number of human rights, some of which are already covered by existing conventions, and others that are not, such as the right of access to public communication for communities, equitable information exchange or a personal presence on the internet.[4] Hamelink's Right to Communicate is thus an extension of existing rights rather than a completely new notion that replaces them.



In its Internet Rights Charter, the Association for Progressive Communications includes a different formulation of the right to communicate, alongside other demands. Under this heading, the Charter lists eight areas in which this right to enjoy the benefits of ICTs can be expressed:

- Access to ICTs
- Inclusion of marginalised groups
- Gender equity
- Affordability
- Developmental impact of internet infrastructure
- Integration with media rights
- Accessibility of public information
- Rights in the workplace.

The Charter is an extensive list of demands meant to guarantee that ICTs be used to promote social justice rather than to increase inequalities. Like Hamelink, it draws on previous attempts to formulate similar demands, such as the People's Communications Charter[5] and A Global Movement for People's Voices in Media and Communication in the 21st Century[6]. In addition to the right to communicate, it refers to other issues such as diversity of content, intellectual property rights, privacy and security, and internet governance.

4 *p cit*; Hamelink, 2002.

5 http://www.pccwaag.org/pcc

6 http://www.comunica.org/v21/statement.htm

The essential human rights of a Declaration on the Right to Communicate:

*INFORMATION RIGHTS such as:

- The right to freedom of thought, conscience and religion
- The right to hold opinions
- The right to express opinions without interference by public or private parties
- The right of people to be properly informed about matters of public interest
- The right of access to information on matters of public interest (held by public or private sources)
- The right to access public means of distributing information, ideas and opinions.

*CULTURAL RIGHTS such as:

- The right to promote and preserve cultural diversity
- The right to freely participate in the cultural life of one's community
- The right to practise cultural traditions
- The right to enjoy the arts and the benefits of scientific progress and its applications
- The right to the protection of national and international cultural property and heritage
- The right to artistic, literary and academic creativity and independence
- The right to use one's language in private and public
- The right of minorities and indigenous people to education and to establish their own media.

*PROTECTION RIGHTS such as:

- The right of people to be protected against interference with their privacy by the media of mass communication, or by public and private agencies involved with data collection.
- The protection of people's private communications against interference by public or private parties
- The right to respect for the standard of due process in forms of public communication
- The right of protection against forms of communication that are discriminatory in terms of race, colour, sex, language, religion or social origin
- The right to be protected against misleading and distorted information
- The right of protection against the systematic and intentional propagation of the belief that individuals and/or social groups deserve to be eliminated
- The right of the protection of the professional independence of employees of public or private communication agencies against the interference by owners and managers of these institutions.

*COLLECTIVE RIGHTS such as:

- The right of access to public communication for communities
- The right to the development of communication infrastructures, to the procurement of adequate resources, the sharing of knowledge and skills, the equality of economic opportunities, and the correction of inequalities
- The right of recognition that knowledge resources are often a common good owned by a collective
- The right of protection of such resources against their private appropriation by knowledge industries.

*PARTICIPATION RIGHTS such as:

- The right to acquire the skills necessary to participate fully in public communication
- The right to people's participation in public decision making on the provision of information, the production of culture or the production and application of knowledge
- The right to people's participation in public decision making on the choice, development and application of communication technology.

Source: Hamelink, 2002.

The Communication Rights in the Information Society (CRIS) campaign[7], a coalition of various groups involved in internet and media activism, has produced a further set of demands[8], grouped together as the right to communicate. This is regarded as "a means to enhance human rights and to strengthen the social, economic and cultural lives of people and communities." The demands are similar to other formulations, and focus on four areas (see box for details):

- Democracy in media and ICTs
- Intellectual property rights
- Civil and political rights
- Equitable and affordable access.

There have been many objections to the idea of a right to communicate. It has been described as so broad as to

CRIS's Vision of the Right to Communicate

Our vision of the 'Information Society' is grounded in the Right to Communicate, as a means to enhance human rights and to strengthen the social, economic and cultural lives of people and communities. Crucial to this is that civil society organisations come together to help build an information society based on principles of transparency, diversity, participation and social and economic justice, and inspired by equitable gender, cultural and regional perspectives.

The Four CRIS Pillars

A. Creating spaces for democratic environments

The public sphere is where civil society defines and renews its understanding of itself in its diversity, and in which political structures are subjected to scrutiny and debate and ultimately held to account for their actions. Core characteristics of the public sphere include freedom of speech, access to information, a healthy public domain and a free and undistorted media and communication regime.

Goals: To reverse trends toward concentration of ownership and control of media - To reclaim the airways and spectrum as public commons and to tax commercial use for public benefit - To promote and sustain alternative, truly independent media and public service media, and advance pluralism against government or private monopoly - To promote freedom of information legislation in public and corporate realms.

B. Reclaiming the use of knowledge and the public domain

Today, copyright is a tool of corporate interests to control ever more of people's knowledge and creativity, including software, denying both creators and society. Globally the WTO and WIPO police the regime with an iron hand, while wealthy countries extract payments from the poor for using knowledge already prised at birth from its creators.

Goals: To secure a full review of copyright globally and nationally, and rebuild it as a flexible and adaptable regime geared to enhancing development and supporting creativity - To nurture and promote 'development-friendly' approaches to intellectual creativity e.g. open source, Copyleft, collective ownership.

C. Reclaiming civil and political rights in the information society

Moves to weaken judicial oversight and accountability, the erosion of long standing data protection principles, legal protections and civil liberties, excessive data retention, surveillance and monitoring of online environments on the pretext of combating 'cyber crime' and 'terrorism', every day diminish our personal freedoms to communicate and deliver ever growing control to governments and corporations.

Goals: To ensure that the 'information society' expands rather than erodes people's rights to privacy, freedom of expression, communication and association.

D. Securing equitable and affordable access

The majority of the world's people lack access to the infrastructure and tools needed to produce and communicate information and knowledge in the information society. Many initiatives, including the WSIS, aim to address this. They usually rest on assumptions that universal access to ICTs will be achieved through market-driven solutions and that more widespread access will necessarily contribute to poverty alleviation and the attainment of the Millennium Development Goals. We question these assumptions.

Goals: To lobby for equitable and affordable access to ICTs for **all** people, specifically the marginalized such as women, the disabled, indigenous people and the urban and rural poor - To promote access as a fundamental right to be realised in the public domain and not dependent on the market forces and profitability - To secure access to information and knowledge as tools for empowerment - To outline and pursue the conditions for securing access not just to ICTs but to information societies as a whole, in a way that is financially, culturally, and ecologically sustainable.
In support of these, we, as signatories to this charter, agree to participate in and cooperate with the international CRIS campaign in debating, writing and disseminating information, and to act together in our respective countries and internationally.

7 http://www.crisinfo.org/live/index.php?section=5

8 http://www.crisinfo.org/live/index.php?section=3&subsection=2

be meaningless, it has been suggested that it would undermine the UDHR, that governments would abuse it, that it would meet so much opposition that it is useless to try to promote it. In a detailed critique of the idea of the right to communicate, the global organisation for freedom of expression, Article 19, claims that this right is not new, but rather a collection of related human rights already expressed in existing conventions.[9]

Towards a perspective on the Right to Communicate

Different rationales have been expressed to support formulation of a new or emerging right to communicate. In a broad sense, its advocates appear to act out of a concern that increasingly, the media are becoming homogenized and minority or dissenting voices are rarely heard.

Globalisation and commercialization of the media is one of the chief concerns: it is argued that in countries around the world, threats from the private sector–such as large media corporations–are as harmful to the right to freedom of expression as traditional state threats. Whilst in many African countries, it is the state which is the problem by imposing restrictive rules and regulations on freedom of expression or by itself dominating the media sector while failing to reflect the diversity that exists within its territory.

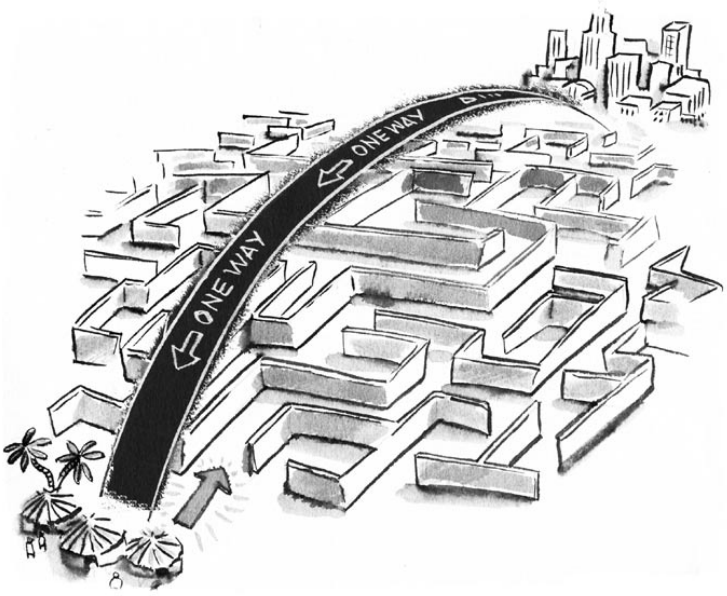
The formulation at the international level of a right to communicate, it is said, would remedy both of these problems. Legal recognition of a right to communicate would additionally help bridge the growing digital divide by empowering those currently left behind in the communications revolution.

However, there appears to be little agreement on the precise definition or content of the right to communicate. How is it different from the right to freedom of expression or to what extent such a right or a Declaration would fit in the existing international Bill of Rights (formed by the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights)?

Source: J Barker and P Noorlender, *FreePress magazine* (April 2003) of the Media Institute of Southern Africa, also available at: http://www.dgroups.org/groups/IS/index.cfm?op=dsp_resource_details&resource_id=3169&cat_id=2779

In the UN, and especially UNESCO, communication rights have had a stormy history, having been associated with a movement for a New World Information and Communication Order (NWICO). This arose in the 1970s, when many poor and third world political elites, seeking to free themselves of the cultural and political legacy of colonial rule, regarded notions of free press and information flow as a disguise for on-going domination by western capitalist countries, and a form of cultural imperialism.

In this context, the 'free flow' of ideas defended by the West was seen as a rationale for a one-way flow of information, from the rich to the poor. Control over information and means of communication were seen as an essential part of the struggle for development and for national and cultural independence. Third World countries called for a balanced flow of information, whereby their own reality could be reflected in the films, news services, TV and other media, and demanded some way of controlling these. They were accused, in turn, of proposing government control over media, and in the process stifling the freedom of speech. The NWICO, coupled with proposals for a New International Economic Order (NIEO), led the USA and the UK to leave UNESCO and withdraw their financial contribution, resulting in a subsequent reduction in its budget and effectiveness.



It is clear that today's formulations of the right to communicate are very different from those in the 1970s and 1980s[10]. For a start, they come not from governments but from civil society. They do not call for restrictions on the freedom of the press, nor for an increased role for governments in regulating the flow of information. The

9 Statement on the Right to Communicate', http://www.article19.org/ViewArticle.asp?AreaID=33&SubAreaID=87&PageID=81&ElementID=53&ArticleID=1394&Comment=1

10 Some of these are documented at http://www.righttocommunicate.org/

emphasis is on empowering individuals and communities. On the other hand, behind both the new and the old formulations is the belief that global media inequalities are fundamental in perpetuating the gap between the rich and the poor. Whereas such inequalities were regarded as a form of neo-colonialism, or cultural imperialism previously, now it is globalisation that has become the new culprit. In this context, the right to freedom of expression appears to mean little if the structure of the media does not allow individuals to be heard outside the walls of their houses.

The proposals for the recognition of communication rights include the right to access communication infrastructure, such as internet access or community media facilities, as a fundamental human right. In this way it takes into account the new ICTs and places social justice and equality in centre stage. In fact, it may be that only now is it possible to demand real communication rights, because we now have technology that allows access for all, an interactive dialogue instead of a one-way process, and the capacity to connect cheaply and effectively with the rest of world's citizens. These proposals recognise the close links with, and parallel situations in, traditional forms of media, extending their demands to the written press, radio, TV, etc. They make it clear that the right to communicate is based on existing human rights and in no way contradicts them; in fact it extends them to cover the new forms of media made possible by new technologies.

appendices / part 5

25. Organisations active in ICT policy (including civil society organisations)

Organisation	URL	Country/region	Region
Democracy Egypt	http://www.democracy-egypt.org	Egypt	Africa
Human Rights Watch Egypt	http://www.hrw.org/mideast/egypt.php	Egypt	Africa
The Egyptian Organization for Human Rights	http://www.eohr.org/	Egypt	Africa
African Telecommunications Union (ATU)	http://www.atu-uat.org/	Kenya	Africa
REGNEC – Senegales WSIS CS group		Senegal	Africa
Bridges.org	http://www.bridges.org	South Africa	Africa
ISOC-ZA	Http://www.isoc.org.za	South Africa	Africa
Media Institute of Southern Africa (MISA)	http://www.misanet.org/	South Africa	Africa
SA ISPA	http://www.ispa.org.za	South Africa	Africa
Australian Copyright Council	http://www.copyright.org.au/	Australia	Asia-Pacific
Australian Digital Alliance (ADA)	http://www.digital.org.au/	Australia	Asia-Pacific
Australian Libraries Copyright Committee	http://www.digital.org.au/alcc/	Australia	Asia-Pacific
Australian Privacy Foundation	http://www.privacy.org.au/	Australia	Asia-Pacific
Electronic Frontiers Australia	http://www.efa.org.au/	Australia	Asia-Pacific
Free Burma Coalition	http://www.freeburmacoalition.org	Burma	Asia-Pacific
Human Rights In China	http://www.hrichina.org	China	Asia-Pacific
Bytesforall	http://www.bytesforall.org	India	Asia-Pacific
Submit Comments on NZ â+~DMCA	http://zork.net/pipermail/free-sklyarov/2002-December/005389.html	New Zealand	Asia-Pacific
Singapore Window	www.singapore-window.org	Singapore	Asia-Pacific
Sintercom	http://www.geocities.com/newsintercom	Singapore	Asia-Pacific
Think Centre	http://www.thinkcentre.org	Singapore	Asia-Pacific
Base21	http://base21.org/base21hot/anticensorship.html	South Korea	Asia-Pacific
Citizens Coalition for Media Watch	http://www.mediawatch.or.kr/	South Korea	Asia-Pacific
Jinbonet and the Progressive Network Center	http://english.jinbo.net	South Korea	Asia-Pacific
Human Rights Society of Uzbekistan Civil Support	http://pougs.boom.ru/news.html	Uzbekistan	Asia-Pacific
Union of Independent Journalists of Uzbekistan	http://www.uiju.org/internet.html	Uzbekistan	Asia-Pacific
(VIBE!AT) - Verein für Internet-Benutzer Austerreichs	http://www.vibe.at/	Austria	Europe
Austrian Association for Internet Users	http://www.vibe.at/	Austria	Europe
Quintessenz	http://www.quintessenz.org/	Austria	Europe

Organisation	URL	Country/region	Region
Verein zur Fürderung Freier Software	http://www.fsf.or.at/	Austria	Europe
Association Electronique Libre	http://www.ael.be/	Belgium	Europe
European Union (EU)	http://europa.eu.int/	Belgium	Europe
Research Center for Computer and Law (CRID)	http://www.droit.fundp.ac.be/crid/default.en.htm	Belgium	Europe
Internet Rights Observatory	http://www.internet-observatory.be/	Belgium	Europe
Applied Research and Communications Fund	http://www.arc.online.bg/main/activ.htm	Bulgaria	Europe
Bulgarian Institute for Legal Development (BILD)	http://www.bild.net/	Bulgaria	Europe
Internet Society Bulgaria (ISOC-Bulgaria)	http://www.isoc.bg/	Bulgaria	Europe
Econnect	http://www.obcan.ecn.cz/	Czech Republic	Europe
Danish Insitute for Human Rights	http://www.humanrights.dk/	Denmark	Europe
Digital Rights Denmark	http://www.digitalrights.dk/	Denmark	Europe
Initiative for Digital Consumer Rights	http://www.digitalforbruger.dk/	Denmark	Europe
SSLUG	http://www.linux-verband.de/	Denmark	Europe
The Danish Institute for Human Rights	http://www.humanrights.dk/	Denmark	Europe
EUROLINUX Alliance	http://eurolinux.org/	Europe	Europe
European Bureau of Library, Information and Documentation Associations	http://www.eblida.org/	Europe	Europe
European Copyright User Platform	http://www.eblida.org/ecup/	Europe	Europe
Copyright (UCUP) Focal Point European Digital Rights	http://www.edri.org/	Europe	Europe
EuroRights	http://www.eurorights.org/	Europe	Europe
Free Software Foundation Europe	http://www.fsfeurope.org/	Europe	Europe
Monitor EU Copyright Directive Status	http://wiki.ael.be/index.php/EUCD-Status	Europe	Europe
Openrevolt.org	http://www.openrevolt.org/	Europe	Europe
Electronic Frontier Finland	http://www.effi.org/index.en.html	Finland	Europe
Association des Utilisateurs d'Internet	http://www.aui.fr/	France	Europe
Association Electronique Libre	http://www.ael.be/	France	Europe
Association Pour la Recherche en Informatique Libre	http://www.april.org/	France	Europe
Council of Europe	http://www.coe.int	France	Europe
EUCD	http://eucd.info/	France	Europe
Europe-Shareware	http://www.europe-shareware.org/	France	Europe
European Telecommunications Standards Institute (ETSI)	http://www.etsi.org	France	Europe
French Speaking Association of Users	http://www.aful.org/	France	Europe

Organisation	URL	Country/region	Region
of Linux and Free Software			
Imaginons un Réseau Internet Solidaire (IRIS)	http://www.iris.sgdg.org/	France	Europe
Institut de Recherche en Propriété Intellectuelle Henri Desbois	http://www.ccip.fr/irp	France	Europe
Organization for Free Software in Education and Teaching	http://www.ofset.org/index.html	France	Europe
Chaos Computer Club	http://www.ccc.de/	Germany	Europe
Deutsche Internet Society (ISOC)	http://www.isoc.de/	Germany	Europe
Förderverein Informationstechnik und Gesellschaft (Fitug)	http://www.fitug.de/	Germany	Europe
Foundation for a Free Information Infrastructure	http://www.ffii.org/index.en.html	Germany	Europe
German Unix User Group	http://www.guug.de/	Germany	Europe
German WSIS Coordinating Group	http://www.worldsummit2003.de/en/nav/14.htm	Germany	Europe
Institut für Rechtsfragen der Freien und Open Source Software (ifrOSS)	http://www.ifross.de/	Germany	Europe
Linux-Verband	http://www.linux-verband.de/	Germany	Europe
Max Planck Institute for Intellectual Property, Competition and Tax Law	http://www.intellecprop.mpg.de	Germany	Europe
Privatkopie	http://www.privatkopie.net/	Germany	Europe
Stop 1984	http://www.stop1984.org/	Germany	Europe
Virtueller Ortsverein der SPD (VOV)	https://www.vov.de/	Germany	Europe
Digital Rights	http://digitalrights.uoa.gr/	Greece	Europe
eDemocracy	http://www.edemokracia.hu	Hungary	Europe
Hungarian Civil Liberties Union	http://www.c3.hu/~hclu/indexuk.htm	Hungary	Europe
Hungarian Civil Liberties Union	http://www.c3.hu/%7Ehclu/indexuk.htm	Hungary	Europe
Hungarian Civil Liberties Union (HCLU)	http://www.tasz.hu	Hungary	Europe
Technika az Emberert Alapitvić+ny (TEA)	http://www.hu.bigbrotherawards.org/	Hungary	Europe
Free Software Foundation India	http://gnu.org.in/	India	Europe
Associazione Software Libero	http://www.softwarelibero.it/	Italy	Europe
Electronic Freedom Italy	http://www.electronicfreedomitaly.org/	Italy	Europe
Electronic Frontiers Italy	http://www.alcei.it/	Italy	Europe
Italian Initiative Against Software Patents	http://nopatents.prosa.it/nopatents	Italy	Europe
Net Jus	http://www.netjus.it/	Italy	Europe
European Parliament	http://www.europarl.eu.int	Luxembourg	Europe
Bits of Freedom	http://www.vosn.nl/	Netherlands	Europe
Buro Jansen & Janssen	http://www.xs4all.nl/%7Erespub/	Netherlands	Europe
Centre for Intellectual Property Law	http://www.law.uu.nl/priv/cier/	Netherlands	Europe

Organisation	URL	Country/region	Region
Institute for Information Law	http://www.ivir.nl/	Netherlands	Europe
Vereniging OpenSource Neederland	http://www.vosn.nl/	Netherlands	Europe
XS4all	http://www.xs4all.nl/	Netherlands	Europe
Electronic Frontier Norway	http://www.efn.no/	Norway	Europe
Norwegian Research Center for Computers and Law	http://www.jus.ui	Norway	Europe
National Association for Free Software (ANSOL)	http://www.ansol.org/ansol.en.html	Portugal	Europe
Moscow Libertarium Forum	http://www.libertarium.ru/libertarium/sorm/	Russia	Europe
Asociación de Internautas	http://www.internautas.org	Spain	Europe
Asociación de Usuarios Españoles de GNU/Linux	http://proinnova.hispalinux.es/	Spain	Europe
Bufet Almeida, Advocats Associats	http://www.bufetalmeida.com/	Spain	Europe
Computer Professionals for Social Responsibility - Spain(CPSR-ES)	http://www.spain.cpsr.org/	Spain	Europe
Kriptopolis	http://www.kriptopolis.com/	Spain	Europe
Pangea	http://www.pangea.org	Spain	Europe
Softcatalá	http://www.softcatala.org	Spain	Europe
Electronic Frontier Sweden	http://www.efs.se/	Sweden	Europe
Swedish Linux User Society	http://www.ch-open.ch/	Sweden	Europe
Association of the Swiss Campaign for the Use of Free Software in Public Adiministration	http://www.wilhelmtux.ch/	Switzerland	Europe
Associazione di Diritto Informatico della Svizzera Italiana (ADISI)	http://www.adisi.ch/	Switzerland	Europe
Linux Users Group Switzerland (LUGS)	http://www.lugs.ch/	Switzerland	Europe
Swiss Civil Society Platform for the World Summit on Information Society	http://www.comunica-ch.net/	Switzerland	Europe
Swiss Internet User Group (SIUG)	http://www.siug.ch/	Switzerland	Europe
Swiss Open Systems User Group (SOSUG)	http://www.ch-open.ch/	Switzerland	Europe
Information Society of Ukraine Foundation	http://www.isu.org.ua	Ukraine	Europe
Internet Rights Ukraine	http://www.internetrights.org.ua	Ukraine	Europe
Association For Free Software	http://www.affs.org.uk/	United Kingdom	Europe
Campaign for Digital Rights	http://ukcdr.org/	United Kingdom	Europe
Cyberrights CyberLiberties	http://www.cyber-rights.org/	United Kingdom	Europe
Foundation for Information Policy Research	http://www.fipr.org/	United Kingdom	Europe
Free Range Activism	http://www.fraw.org.uk/	United Kingdom	Europe
GreenNet	http://www.gn.apc.org	United Kingdom	Europe
Internet Freedom	http://www.netfreedom.org/	United Kingdom	Europe

Organisation	URL	Country/region	Region
Internet Rights UK	http://www.internetrights.org.uk	United Kingdom	Europe
Lonix - The London Linux User Group	http://www.lonix.org.uk/	United Kingdom	Europe
Privacy International	http://www.privacyinternational.org	United Kingdom	Europe
UK Commission on Intellectual Property Rights	http://www.iprcommission.org/	United Kingdom	Europe
United Nations Commission on International Trade Law (UNCITRAL)	htttp://www.uncitral.org	Austria	International
United Nations Educational, Scientific, and Cultural Organization (UNESCO)	http://www.unesco.org/	France	International
World Intellectual Property Organization (WIPO)	http://www.wipo.int	Geneva	International
AfrICANN	http://www.africann.org/	International	International
Association for Progressive Communications	http://www.apc.org/	International	International
Global Business Dialogue on Electronic Commerce (GBDe)	www.gbde.org	International	International
Global Internet Liberty Campaign (GILC)	http://www.gilc.org/	International	International
Human Rights Watch	http://www.hrw.org/advocacy/internet/	International	International
ICANN Watch	http://www.icannwatch.org/	International	International
IFEX	http://www.ifex.org/	International	International
Internet Architecture Board (IAB)	http://www.iab.org	International	International
Internet Engineering Task Force (IETF)	http://www.ietf.org	International	International
Internet Society (ISOC)	http://www.isoc.org/	International	International
IP Justice	http://www.ipjustice.org/	International	International
Organization for Economic Cooperation and Development	http://www.oecd.org	International	International
Stop the Free Trade Area of the Americas (FTAA) Treaty	http://stopftaa.org/new/	International	International
United Nations Information and Communication Technology Taskforce (UN-ICT Taskforce)	http://www.unicttaskforce.org	International	International
World Wide Web Consortium (W3C)	www.w3.org	International	International
International Telecommunications Union (ITU)	http://www.itu.int	Switzerland	International
United Nations Conference on Trade and Development (UNCTAD)	http://www.unctad.org	Switzerland	International
World Trade Organization (WTO)	http://www.wto.org	Switzerland	International
Internet Corporation of Assigned Numbers and Names (ICANN)	http://www.icann.org	USA	International
Internet Society	http://www.isoc.org	USA	International
World Bank	http://www.worldbank.org	USA	International
Fronteras Electrónicas de Argentina	http://www.ulpiano.com/EFA.htm	Argentina	Latin America
Canadian Open Source Education Network	http://www.canopener.ca/	Canada	North America

Organisation	URL	Country/region	Region
Council of Canada	http://www.internetcouncil.ca/	Canada	North America
Digital Copyright in Canada	http://www.lexinformatica.org/copyright/	Canada	North America
Electronic Frontier Canada	http://www.efc.ca/	Canada	North America
Privaterra	http://www.privaterra.org/	Canada	North America
Rights and Democracy	http://www.ichrdd.ca/	Canada	North America
American Civil Liberties Union (ACLU)	http://www.aclu.org/Privacy/PrivacyMain.cfm/	United States	North America
American Library Association (ALA)	http://www.ala.org/	United States	North America
American Society for Information Science (ASIS)	http://www.asis.org/	United States	North America
Anti-DMCA	http://www.anti-dmca.org/	United States	North America
Association for Computing Machinery (ACM)	http://www.acm.org/	United States	North America
Association of Reseach Libraries	http://www.arl.org/	United States	North America
Berkeley Center for Law & Technology	http://www.law.berkeley.edu/institutes/bclt/	United States	North America
Berkman Center for Internet & Society at Harvard Law School	http://cyber.law.harvard.edu/	United States	North America
Center for Democracy and Technology (CDT)	http://www.cdt.org/	United States	North America
Center for Public Domain	http://www.centerforthepublicdomain.org/	United States	North America
Center for the Study of the Public Domain at Duke University School of Law	http://www.law.duke.edu/ip/	United States	North America
Chilling Effects Project	http://www.chillingeffects.org/	United States	North America
Computer & Communications Industry Association (CCIA)	http://www.ccianet.org/	United States	North America
Computer Professionals for Social Responsibility (CPSR)	http://www.cpsr.org/	United States	North America
Consumer Project on Technology	http://www.cptech.org/	United States	North America
Consumers Electronics Association (CEA)	http://www.ce.org/	United States	North America
Copyright Society of the USA	http://www.csusa.org/	United States	North America
Creative Commons	http://www.creativecommons.org/	United States	North America
CryptoRights Foundation	http://www.cryptorights.org/	United States	North America
Digital Consumer	http://www.digitalconsumer.org/	United States	North America
Digital Future Coalition	http://www.dfc.org/	United States	North America
EFF-Austin	http://www.effaustin.org/	United States	North America
Electronic Frontier Foundation (EFF)	http://www.eff.org/	United States	North America
Electronic Privacy Information Center (EPIC)	http://www.epic.org/	United States	North America
First Amendment Project	http://www.thefirstamendment.org/	United States	North America
Free Expression Policy Project	http://www.fepproject.org/index.html	United States	North America

Organisation	URL	Country/region	Region
Free Information Property Exchange	http://www.freeipx.org/	United States	North America
Free Software Foundation (FSF)	http://www.fsf.org/	United States	North America
Future of Music Coalition	http://www.futureofmusic.org/	United States	North America
Home Recording Rights Coalition (HRRC)	http://www.hrrc.org/	United States	North America
Intellectual Property Society	http://www.ipsociety.net/	United States	North America
Motion Picture Industry Association of America (MPAA)	http://www.mpaa.org/	United States	North America
Net Action	http://www.netaction.org/	United States	North America
Online Policy Group	http://www.onlinepolicy.org/	United States	North America
Privacy Activism	http://www.privacyactivism.org/	United States	North America
Protect Fair Use	http://www.protectfairuse.org/	United States	North America
Pubic Knowledge	http://www.publicknowledge.org/	United States	North America
Public Citizen	http://www.citizen.org/	United States	North America
Recording Industry Association of America (RIAA)	http://www.riaa.org/	United States	North America
Stanford Center for Internet and Society	http://cyberlaw.stanford.edu/	United States	North America
The Privacy Coalition	http://www.privacycoalition.org/	United States	North America
Inter-American Telecommunication Commission (CITEL)	http://www.citel.oas.org	United States	North America

26. Glossary

Adware: Like spyware, this is software that installs itself on another computer without the owner's knowledge, and in certain situations places advertisements on the screen

Bandwidth: The amount of information that can be sent through a connection (usually measured in bits-per-second). Bandwidth is the range between the highest and lowest frequencies on a channel; more commonly, the amount of data that can flow through a channel at the same time. In either case, the capacity of a telecommunications channel is measured by its bandwidth.

Blog: Short for Web log, a blog is a Web page that serves as a publicly accessible personal journal for an individual. Typically updated daily, blogs often reflect the personality of the author.

Browser: Short for Web browser, a software used to locate and display Web pages. Most can display graphics and text as well as present multimedia information including sound and video.

Circuit switching: the traditional way of information or electrical flow, where cutting the circuit means the end of the flow. Different from packet switching, where the information is divided up and sent in individual packets, which can find alternative routes to their destination if one route is blocked or cut.

Cookies: A message given to a web browser by a web server. The browser stores the message in a text file. The message is then sent back to the server each time the browser requests a page from the server. The main purpose of cookies is to identify users and possibly prepare customised web pages for them. Web sites use cookies for several different reasons: to collect demographic information about who is visiting the Web site; to personalise the user's experience on the Web site, and; to monitor advertisements. Any personal information that you give to a Web site, including credit card information, will most likely be stored in a cookie unless you have turned off the cookie feature in your browser.

Copyright: A set of specific rights to content use, manipulation, and distribution that the law grants content creators, leaving all other rights to the public. A copyright is an intellectual property protection granted to literary, musical and artistic works, including drawings, poems, films, written publications, and software.

Cryptography: The art of protecting information by transforming it (encrypting it) into an unreadable format, called cipher text. Only those who possess a secret key can decipher (or decrypt) the message into plain text. As the internet and other forms of electronic communication become more prevalent, electronic security is becoming increasingly important. Cryptography is used to protect email messages, credit card information, and corporate data. Cryptography systems can be broadly classified into symmetric-key systems that use a single key that both the sender and recipient have, and public-key systems that use two keys, a public key known to everyone and a private key that only the recipient of messages uses.

Cyberspace: A metaphor for describing the non-physical terrain created by computer systems. Online systems, for example, create a cyberspace within which people can communicate with one another (via email), do research, or simply window shop. Like physical space, cyberspace contains objects (files, mail messages, graphics, etc.) and different modes of transportation and delivery. Unlike real space, though, exploring cyberspace does not require any physical movement other than pressing keys on a keyboard or moving a mouse. The term was coined by author William Gibson in his sci-fi novel *Neuromancer* (1984).

Digital Divide: "Although often framed as an issue of extremes, the digital divide refers to a collection of complex factors that affect whether an individual, social group, country or region has access to the technologies associated with the information economy as well as the educational skills to achieve optimal application of those technologies", from "Analysis of the Digital Divide", Powerpoint presentation, October 2000, http://www.giic.org

Digital Signatures: A digital code that can be attached to an electronically transmitted message that uniquely identifies the sender. Like a written signature, the purpose of a digital signature is to guarantee that the individual sending the message really is who he or she claims to be. Digital signatures are especially important for electronic commerce and are a key component of most authentication schemes. To be effective, digital signatures must be unforgeable. There are a number of different encryption techniques to guarantee this level of security.

Digital Subscriber Lines (DSL): A method for moving data over regular phone lines. A DSL circuit is much faster than a regular phone connection, and the wires coming into the subscriber's premises are the same (copper) wires used for regular phone service. A DSL circuit must be configured to connect two specific locations. They are sometimes referred to as last-mile technologies because they are used only for connections from a telephone switching station to a home or office, not between switching stations.

Encryption: The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it.

Fair Use: a copyright principle based on the belief that the public is entitled to freely use portions of copyrighted materials for purposes of commentary and criticism. For example, if you wish to criticise a novelist, you should have the freedom to quote a portion of the novelist's work without asking permission. Without this freedom, copyright owners could stifle any negative comments about their work.

Fair Dealing: Similar to fair use, used in many common law countries. The main difference is that "fair use" tends to be an open-ended legal doctrine (the US copyright statute provides factors which contribute to fair use), while "fair dealing" is defined in a constrained manner, through an enumerated list of causes for exemption that allows little room for judicial interpretation.

Free Software: Software that gives the user the freedom to run the programme for any purpose, to study how the programme works and adapt it to the user's needs through having access to the source code, to redistribute copies in order to help other users, to improve the programme and release it to the public. Access to the source code is a precondition for this. Free software usually uses the GPL licence to ensure that the software remains free. It is different from open source software in its insistence on the social aspects and the benefits for society of free software.

Freeware: Copyrighted software given away for free by the author. Although it is available for free, the author retains the copyright, which means that you can do nothing with it unless it is expressly allowed by the author. Often the author allows people to use the software, but not sell it.

GPL: Short for General Public License, the license that accompanies some open source software that details how the software and its accompany source code can be freely copied, distributed and modified. One of the basic tenets of the GPL is that anyone who acquires the material must make it available to anyone else under the same licensing agreement. The GPL does not cover activities other than the copying, distributing and modifying of the source code. A GPL is also referred to as a copyleft, in contrast to a copyright that identifies the proprietary rights of material.

Hacker: A slang term for a computer enthusiast, that is a person who enjoys learning programming languages and computer systems and can often be considered an expert on the subject. The term is popularly used to refer to individuals who gain unauthorised access to computer systems for the purpose of stealing and corrupting data. Hackers themselves maintain that the proper term for such individuals is cracker.

Information and Communications Technology (ICT): "The means of generating, processing, transporting and presenting information" (OECD).

Intellectual property: Intellectual property (IP) is an intangible thing (you cannot touch it or hold it in your hand) that you can own, similar to the way that you can own tangible things like a car or a plot of land. It can be something that you have written, drawn, designed, invented, or spoken, and it can be something that you have created yourself or paid someone to create for you. Like tangible property, you can buy, sell, exchange or give away intellectual property, and you can control its use by others. However, in order for your intangible thing to qualify as intellectual property so you can gain these rights, you have to be able to distinguish it from similar things. The concept of intellectual property is intended to protect innovations and allow people to make money by selling their ideas. Usually the expression 'intellectual property' is used as a legal term to indicate four distinct types of protection given to intangible property: patents, trademarks, copyrights, and trade secrets.

Interconnection: The linking together of systems. The linkage used to join two or more communications units, such as systems, networks, links, nodes, equipment, circuits, and devices.

Internet: A worldwide interconnection of individual networks operated by government, industry, academia, and private parties. *Note:* The internet originally served to interconnect laboratories engaged in government research, and has now been expanded to serve millions of users and a multitude of purposes.

Internet backbone: This super-fast network spanning the world from one major metropolitan area to another is provided by a handful of national internet service providers (ISPs). These organisations (including Net 99 and Alternet) use connections running at approximately 45 mbps (T3 lines) linked up at specified interconnection points called national access points (which are located in major metropolitan areas). Local ISPs connect to this backbone through routers so that data can be carried though the backbone to its destination. http://www.cnet.com/Resources/Info/Glossary/Terms/internetbackbone.html

Internet Exchange Point (IXP): A physical network infrastructure operated by a single entity with the purpose of facilitating the exchange of internet traffic between ISPs.

Internet Service Provider (ISP): A company that provides access to the internet for companies or individuals.

Internet protocol (IP): A standard protocol designed for use in interconnected systems of packet-switched computer communication networks. *Note:* The internet protocol provides for transmitting blocks of data called datagrams from sources to destinations, where sources and destinations are hosts identified by fixed-length addresses. The internet protocol also provides for fragmentation and reassembly of long datagrams, if necessary, for transmission through small-packet networks. http://www.its.bldrdoc.gov/fs-1037/

Local Area Network (LAN): A technique by which many computers in the same physical location can be linked together to communicate or share resources. LANs may be linked to the internet, or they may be self-contained.

Log: Computers, especially servers, keep a record of the machine's activity, normally in a text file that can be read later. This log can be referenced to find out, for example, who accessed the server and when, with which IP number, what happened at which time, error messages, etc.

MAE: The MCI MAE® Internet Exchange Facilities are the access points where ISPs may interconnect. A significant amount of the traffic that flows between ISP networks passes through the MAE exchanges. ISPs subscribe ports on switches in the MAE facilities and the circuits leading into those ports.

NAP: Network Access Point, a point in the routing hierarchy of the Internet that exchanges traffic between major backbones. First proposed by the NFS when it commercialised the internet.

Network: Any time you connect two or more computers together so that they can share resources, you have a computer network. Connect two or more networks together and you have an internet.

Open Source Software: Software for which the underlying programming code is available to the users so that they may read it, make changes to it, and build new versions of the software incorporating their changes. There are many types of Open Source Software, mainly differing in the licensing term under which (altered) copies of the source code may (or must be) redistributed.

Packets: A piece of a message transmitted over a packet-switching network. See under *packet switching*. One of the key features of a packet is that it contains the destination address in addition to the data.

Packet Switching: The method used to move data around on the internet. In packet switching, all the data coming out of a machine is broken up into chunks, each chunk has the address of where it came from and where it is going. This enables chunks of data from many different sources to mingle on the same lines, and be sorted and directed along different routes by special machines along the way.

Patent: A patent is an intellectual property protection that applies to inventions or designs for inventions, which gives the inventor exclusive rights to make, use, and sell the invention for a certain period of time.

Peer to Peer Networks: Often referred to simply as *peer-to-peer*, or abbreviated p*2p*, a type of network in which each workstation has equivalent capabilities and responsibilities. This differs from client/server architectures, in which some computers are dedicated to serving the others. Peer-to-peer networks are generally simpler, but they usually do not offer the same performance under heavy loads.

Portal (Web Portal): A Web site that is or is intended to be the first place people see when using the Web. Typically a Portal site has a catalogue of web sites, a search engine, or both. A Portal site may also offer email and other service to entice people to use that site as their main point of entry (hence 'portal') to the Web.

Price cap regulation: price cap regulation involves regulating the cost to consumers of telecommunication services rather than regulating the companies' profit. It was first introduced when British Telecom was privatised in 1984. By limiting prices that companies can charge and allowing them to keep profit earned by operating within the cap, price cap regulation is thought to provide an incentive to increase efficiency and productivity. Summarised from CSE: Citizens for a Sound Economy - Issue Analysis 85 – *Primer on Price Cap Regulation.*

Privatisation: the process whereby functions that were formerly run by the government are delegated instead to the private sector. Privatisation occurs when the government sells a government owned business or service to private interests. This is usually the first step in creating a competitive market for the good or service that the government owned business previously had a monopoly on.

Proxy: A server that sits between a client application, such as a Web browser, and a real server. It intercepts all requests to the real server to see if it can fulfil the requests itself. If not, it forwards the request to the real server. Proxy servers have two main purposes. They can dramatically improve performance for groups of users, because they save the results of all requests for a certain amount of time. Proxy servers can also be used to filter requests.

Shareware: Software distributed on the basis of an honour system. Most shareware is delivered free of charge, but the author usually requests that you pay a small fee if you like the programme and use it regularly. By sending the small fee, you become registered with the producer so that you can receive service assistance and updates. You can copy shareware and pass it along to friends and colleagues, but they too are expected to pay a fee if they use the product.

Spam: Electronic junk mail or junk newsgroup postings. In addition to wasting people's time with unwanted email, spam also eats up a lot of network bandwidth. Consequently, there are many organisations and individuals, who have taken it upon themselves to fight spam with a variety of techniques. But because the internet is public, there is really little that can be done to prevent spam, just as it is impossible to prevent junk mail.

Spyware: Spyware is any software that covertly gathers user information through the user's internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programmes that can be downloaded from the internet. Once installed, the spyware monitors user activity on the internet and transmits that information in the background to someone else. Spyware can also gather information about email addresses and even passwords and credit card numbers. Spyware is similar to a Trojan horse in that users unwittingly install it when they install another product. A common way to become a victim of spyware is to download certain peer-to-peer file swapping products that are available today.

Aside from the questions of ethics and privacy, spyware steals from the user by using the computer;s memory resources and also by eating bandwidth as it sends information back to the spyware's home base via the user's internet connection. Because spyware is using memory and system resources, the applications running in the background can lead to system crashes or general system instability.

Telecentre: There are many different types of telecentres but essentially a telecentre is a physical location where community members have access to ICT hardware, information, a range of social and economic enhancement services, and support systems that facilitate economic and social sustainability of the telecentre itself. The aim of most telecentre projects is to provide public access to ICT and related services for a community that does not have widespread access.

Telecommunications: All types of data transmission, from voice to video

Universal Service: The concept of making basic local telephone service (and, in some cases, certain other telecommunications and information services) available at an affordable price to all people within a country or specified jurisdictional area. http://www.its.bldrdoc.gov/fs-1037/

Also defined as affordable access to and effective use of the Internet. (O'Siochru)

Voice Over IP (VOIP): Hardware and software that enable people to use the internet as the transmission medium for telephone calls. For users who have free, or fixed-price internet access, internet telephony software provides free telephone calls anywhere in the world.

3G: 3G is an ITU specification for the third generation (analogue cellular was the first generation, digital Personal Communications Services – PCS - the second) of mobile communications technology. 3G promises increased bandwidth.

27. Bibliography

African Information Society Initiative (AISI), *An Action Framework to Build Africa's Information and Communication Infrastructure*, http://www.uneca.org/aisi/aisi.htm#gender

Africa Internet Forum, *Economic Toolkit for African Policymakers*, UNECA and infoDev project, http://www.infodev.org

Akash Kapur, *Why ICANN Needs Fresh Blood: A Deeper View*, 26 March 2003, http://www.circleid.com/artcles/2580.asp

APC, *FAQ About Conducting a National WSIS Consultation*, http://rights.apc.org/nationalfaq_wsis_v1.pdf

APC, *Africa ICT Policy Monitor*, http://africa.rights.apc.org

APC, *Derechos en Internet en America Latina and the Carribean*, http://lac.derechos.apc.org

APC, *Documenting 10 years of Challenge and Innovation: the APC Annual Report 2000*, http://www.apc.org/books/apc_annualreport_2002.zip

APC, *European Civil Society Internet Rights Project*, http://europe.rights.apc.org

APC, *ICT Policy for Civil Society: Training Curriculum*, http://www.apc.org/english/capacity/policy/curriculum.shtml

APC, *Participating With Safety*, http://secdocs.net/manual/lp-sec/

APC, *APC Africa Women*, http://www.apcafricawomen.org

APC & CRIS, *Involving Civil Society in ICT Policy: The Wsis*, APC, 2003

APC, *Internet Rights Charter*, http://www.apc.org/english/rights/charter.shtml

APC WNSP, *Gender Evaluation Methodology (GEM)*, http://www.apcwomen.org/gem

APC WNSP, *Information and Communication Technologies for Social Change*, http://www.apcwomen.org/gem/icts.htm

APC WNSP, *Information and Communication Technologies: A Women's Agenda*, http://www.apcwomen.org/work/policy/women-rights.html

APC WNSP, *Gender and Information Technology: The Right of Women to Have Equal Access to Computer Communications Technology and Networks*, http://www.apcwomen.org/work/policy/gender-ict-unwcw.html

Bell, R, *The Halfway Proposition*, http://www.afrispa.org/Initiatives.htm

Campbell, D, *Interception Capabilities 2000*, PERLINK http://www.cyber-rights.org/interception/stoa/interception_capabilities_2000.htm

Castells, M, *The Rise of the Network Society*, Blackwell, 2000

Castells, M, *Information Technology, Globalization and Social Development*, 1999, http://www.unrisd.org/unrisd/website/document.nsf/(httpPublications)/F270E0C066F3DE7780256B67005B728C?OpenDocument

Castells, M & Ince, M, *Conversations with Manuel Castells*, Polity, 2003

Commonwealth Telecommunications Organisation & Panos, *Louder Voices: Strengthening Developing Country Participation in International ICT Decision-making*, July 2002

Creative Commons, http://creativecommons.org/

CRIS. Campaign, *Issue Papers*, http://www.crisinfo.org/live/index.php?section=4

DFID, *Internet Costs Study*, http://www.clairemilne.btinternet.co.uk/telecommunications_development/DFID_internet_cost_report.htm

Dogan, P, *Vertical Relations and Connectivity in the Internet*, in *Communications and Strategies*, 47, 2002, pp. 87-101

Dutta, S, Lanvin, B & Paua F (eds) *Global Information Technologies Report 2002/2003, Readiness for the Networked World*, Oxford University Press, 2003

EPIC, *Faulty Filters: How Content Filters Block Access to Kid-Friendly Information on the Internet*, http://www.epic.org/reports/filter-report.html

Patrick Farajian, *Key Lessons in Telecommunications Reform*, Economic Commission for West Asia, West Asia Preparatory Conference for the World Summit on the Information Society, February 2003

Gromov, G, *The Roads and Crossroads of Internet History*, http://www.netvalley.com/intval1.html

Haaretz Daily, "Big Brother is Watching You – and Documenting", 10/8/2003

Hamelink, C, *The Right to Communicate*, presented at Prepcom1, (2002), http://www.geneva2003.org/home/events/documents/gen_hamelink_en.htm

Hamelink, C, *Human Rights for the Information Society*, Briefing Paper Series for the WSIS (UNRISD), 2003

Hunter, C A, *The Real History of the Internet*, http://www.asc.upenn.edu/usr/chunter/agora_uses/chapter_2.html

Hughes, D, *Globalization, Information Technology, and Sexual Exploitation of Women and Children*, Rain and Thunder – A Radical Feminist Journal of Discussion and Activism, 13, Winter 2001, http://www.uri.edu/artsci/wms/hughes/globe.doc

Hughes, D, *The Use of New Communications and Information Technologies for Sexual Exploitation of Women and Children*, Hastings Women's Law Journal, 13:1, http://www.uri.edu/artsci/wms/hughes/new_tech.pdf

Huston, G, *Interconnection, Peering and Settlements*, Telstra Australia, http://www.potaroo.net/papers.html or http://www.uixp.co.ug/interconnect.html

International Charging Arrangements for Internet Services (ICAIS), http://www.apectelwg.org

ITU, *The African Internet and Telecom Summit*, http://www.itu.int/africainternet2000/

ITU, *Asia Pacific Telecommunication Indicators*, 2002.

ITU, *Effective Regulation: Trends in Telecommunications Reform*, 2002

ITU, *World Telecommunication Development Report*, 2002

Intven, H, (ed), *Telecommunications Regulation Handbook*, World Bank, 2001

James, T, (ed), *An Information Policy Handbook for Southern Africa*, IDRC, 2001, http://www.apc.org/books/ictpolsa/index.html

Massel, G, http://www.ispmap.org.za

McPhail, T. M, *Global communication*, Allyn & Bacon, 2002

Naughton, J, "China's Great Net Firewall Fans Flames of Censorship", *The Observer*, 8/12/2002, http://observer.guardian.co.uk/business/story/0,6903,855769,00.html

Norman, P, *Policing High Tech Crime in the Global Context*, http://www.bileta.ax.uk/99papers/morman.htm

Nam, H & Kim, I, *Digital Environment and Intellectual Property Rights*, Asian Internet Rights Conference, Jinbonet, 2001

Reddy, S, *Can ICANN Meet the Needs of Less Developed Countries?* May 20, 2003, http://www.circleid.com/articles/2595.asp

O'Siochru, S, *Universal Service, Policy and Regulation - A Review of Experience Internationally*, IDRC, 1996

O'Siochru, S, Girard, B & Mahan, A, *Global Media Governance*, Rowan & Littlefield, 2002

OECD, *Broadband Access for Business*, 2002

OECD, *Netcraft* by Brian Longwe

Prahalad, C K & Hammond A, *Serving the World's Poor, Profitably*, Harvard Business Review, Reprint R0209C

Rowe, A, *Green Backlash: Global Subversion of the Environmental Movement*, Routledge, 1996

Stallman, R, *Free Software Free Society*, GNUPress, 2002

Stanford University Libraries, *Copyright and Fair Use*, http://fairuse.stanford.edu/index.html

UNDP, *Human Development Report*, 2001

UNECE, *Towards a Knowledge Based Economy*, (2002)

UNIFEM, *Tracking Regional Progress towards Implementation of the Beijing Platform for Action*, http://www.unifem.undp.org/beijing/regional_progress.html

United Nations, *The World's Women 2000: Trends and Statistics*, 2000

Wikipedia, http://www.wikipedia.org/

WITSA papers, http://www.witsa.org/papers/

WomenAction, http://www.womenaction.org/

Women'sNet, http://www.womensnet.org.za

World Summit on the Information Society (WSIS), *Gender Caucus* website hosted by the Women of Uganda Network, S/wsisgc.html" http://www.wougnet.org/WSIS/wsisgc.html

WSIS Civil Society, *Seven Musts*, http://www.worldsummit2003.de/download_de/WSIS-SCT-7Musts-25Feb2003.rtf