INFORMATION AND COMMUNICATION TECHNOLOGIES AND HUMAN RIGHTS
Abstract

The rapid evolution of information and communications technology (ICT) and associated digital communications over the past two decades has dramatically changed communication practices across the world. This has had profound implications for human rights on a number of levels. Firstly, communication technologies are presenting new ways to more fully realise our human rights. This is particularly true of the right to freedom of expression. Secondly, ICTs have provided human rights activists with new tools for defending human rights. Internet access via mobile phones gives citizens the power to communicate rights violations in real time to global audiences; social networking tools connect human rights defenders across the world to enhance collaboration and information sharing; censorship circumvention technologies allow people to bypass attempts to monitor and control information and communication flows. However, as well as unleashing tremendous new opportunities for protecting and advancing human rights, digital communications also present a series of serious challenges. These include direct threats to human rights, such as the development of increasingly sophisticated censorship and surveillance mechanisms. They also include deeper, structural problems such as the persistence of digital divides in access to communications infrastructure and capacities along geographical, gender and social lines.
This study was requested by the European Parliament’s Committee on Subcommittee on Human Rights.

**AUTHOR(S):**

Lisa HORNER, Head of Research and Policy, Global Partners and Associates, LONDON, UNITED KINGDOM
Dixie HAWTIN, Global Partners and Associates, LONDON, UNITED KINGDOM
Andrew PUDDEPHATT, Director, Global Partners and Associates, LONDON, UNITED KINGDOM

**ADMINISTRATOR RESPONSIBLE:**

Jarmo OIKARINEN
Directorate-General for External Policies of the Union
Policy Department
WIB 06 M 71
rue Wiertz 60
B-1047 Brussels

**LINGUISTIC VERSIONS**

Original: EN

**ABOUT THE EDITOR**

Editorial closing date: 14 June 2010.
© European Parliament, [2010]
Printed in [Belgium]

The study is available on the Internet at

If you are unable to download the information you require, please request a paper copy by e-mail: xp-poldep@europarl.europa.eu

**DISCLAIMER**

Any opinions expressed in this document are the sole responsibility of the author and do not necessarily represent the official position of the European Parliament.

Reproduction and translation, except for commercial purposes, are authorised, provided the source is acknowledged and provided the publisher is given prior notice and supplied with a copy of the publication.
TABLE OF CONTENTS

LIST OF BOXES....................................................................................................................................................... 5
LIST OF FIGURES.......................................................................................................................................................... 6
EXECUTIVE SUMMARY .................................................................................................................................................. 7
1 INTRODUCTION .......................................................................................................................................................... 12
  1.1 Setting the Scene.................................................................................................................................................. 12
  1.2 The transformative and disruptive nature of digital communications ............................................................... 13
  1.3 Opportunities and challenges for human rights: an overview of the issues ....................................................... 15
  1.4 The “layer model” of digital communication environments: an analytical tool .................................................. 16
  1.5 Cross cutting issues............................................................................................................................................... 18
  1.5.1 Balancing human rights on the internet ........................................................................................................... 19
  1.5.2 Intermediary Liability ........................................................................................................................................ 20
  1.6 The key message .................................................................................................................................................. 22
2 FREEDOM OF EXPRESSION, CENSORSHIP AND CONTROL........................................................................... 23
  2.1 Freedom of expression as a foundation right ..................................................................................................... 23
  2.2 Democratising freedom of expression through digital communications ............................................................ 24
  2.3 The illegal censorship of legitimate speech online .............................................................................................. 25
  2.3.1 Online censorship mechanisms ...................................................................................................................... 25
  2.3.2 An International snapshot of censorship practices .......................................................................................... 28
  2.3.3 The EU response .............................................................................................................................................. 30
  2.3.4 Roles and responsibilities of the corporate sector ............................................................................................ 31
  2.4 Legitimate regulation of speech online ............................................................................................................... 34
  2.4.1 Balancing civil rights with children’s rights online .......................................................................................... 34
  2.4.2 Regulating hate speech ...................................................................................................................................... 36
  2.4.3 The roles and responsibilities of the corporate sector ...................................................................................... 37
  2.5 Expanding the public interest dimensions of digital communications .............................................................. 38
  2.6 Conclusions ......................................................................................................................................................... 40
3 PRIVACY, SECURITY AND SURVEILLANCE: THE NEED FOR BALANCE .............................................. 41
  3.1 Privacy within the international human rights framework .................................................................................... 42
  3.2 Challenges to privacy: enhanced surveillance and data collection ........................................................................ 42
  3.2.1 Enabling the collection and monitoring of increasing volumes of personal information ................................ 42
  3.2.2 Assisting in the consolidation and analysis of personal information ............................................................... 43
  3.2.3 The difficulties of protecting personal data in the digital age .......................................................................... 44
  3.3 The use of personal data for commercial purposes ............................................................................................. 45
  3.3.1 Privacy concerns over the activities of internet intermediaries ..................................................................... 45
  3.3.2 Privacy and data protection regulation ........................................................................................................... 47
  3.4 Surveillance and data protection to increase public security ................................................................................ 48
  3.4.1 Cyber-extremism and terrorism ....................................................................................................................... 49
  3.4.2 Cybercrime ....................................................................................................................................................... 50
  3.4.3 State-sponsored Cyber-Attacks ....................................................................................................................... 50
  3.4.4 Promoting a safe and open internet: the need for balance and proportionality ........................................... 50
LIST OF BOXES

Box 1: Filtering Mechanisms ..................................................................................................................................26
Box 2: Censorship in China ......................................................................................................................27
Box 3: Google in China ........................................................................................................................32
Box 4: Who is responsible for illegal content online? ................................................................................38
Box 5: Article 15, UN International Covenant on Economic, Social and Cultural Rights (1966) ...53
Box 6: Common forms of DRM ...................................................................................................................56
Box 7: Alternatives to traditional copyright enforcement ..............................................................................62
LIST OF FIGURES

Figure 1 - Changes in access to communications platforms, 1998-2009
(Source: ITU, 2010)............................................................................................................................. 14

Figure 2 - A layer model of digital networked communications .................................................... 18

Figure 3 - The first map shows the countries of the world according to their geographical area. The second map is distorted to show the proportion of worldwide net exports of royalties and license fees that originate there, based on 2005 UNCTAD figures (in US$). Source: World Mapper (http://www.worldmapper.org/display.php?selected=99#)................................................................. 60
EXECUTIVE SUMMARY

The rapid evolution of information and communications technology (ICT) and associated digital communications over the past two decades has dramatically changed communication practices across the world. The internet and mobile phones have opened up new horizons for communication, connecting people to a global network for sharing information and ideas. This has had profound implications for human rights on a number of levels.

Firstly, communication technologies are presenting new ways to more fully realise our human rights. This is particularly true of the right to freedom of expression, with ICTs enhancing our ability not only to receive information, but also to actively seek and impart it. Digital communications are spurring the development of empowering spaces for communication, collaboration and exchange. As well as enhancing many civil and political rights, ICTs also offer new potential for realising economic, social and cultural rights through providing people with new channels for accessing and improving public services, markets for trade and commerce, and global knowledge resources.

Secondly, ICTs have provided human rights activists with new tools for defending human rights. For example: internet access via mobile phones gives citizens the power to communicate rights violations in real time to global audiences; social networking tools connect human rights defenders across the world to enhance collaboration and information sharing; censorship circumvention technologies allow people to bypass attempts to monitor and control information and communication flows.

However, as well as unleashing tremendous new opportunities for protecting and advancing human rights, digital communications also present a series of serious challenges. These include direct threats to human rights, such as the development of increasingly sophisticated censorship and surveillance mechanisms. They also include deeper, structural problems such as the persistence of digital divides in access to communications infrastructure and capacities along geographical, gender and social lines.

This report was commissioned by the European Parliament’s Subcommittee on human rights to examine these opportunities and challenges, highlighting areas in which the European Union could play a positive role in building digital communications environments that protect and expand human rights.

Setting the scene

The first chapter of the report provides an introduction to the issues. It highlights the transformative and disruptive nature of digital communications, demonstrating how they have presented tremendous opportunities for democratising freedom of expression itself. Digital communications have empowered people to communicate directly with each other, rather than having to go through gatekeepers such as government spokespeople and the mass media. The changes that they have wrought on society are comparable to the impact of the invention of the Gutenberg press.
The report presents a framework for examining and understanding the policy intersection between human rights and digital communications. In the past, human rights activists were concerned primarily with the content of communication and whether it was being directly censored. However, in digital networks, the nature and architecture of communications infrastructure and protocols have a strong influence on communications content, capacities and possibilities. It is therefore necessary to consider challenges and opportunities for human rights at four broad layers of digital communications environments: the physical infrastructure; the connectivity and protocols that allow devices to talk to one another; the applications that we use to create, access and navigate content; and the communications content itself. Subsequent chapters of the report use this framework to examine the relationship between ICTs and human rights.

Two significant cross cutting issues emerge throughout the report. The first is the challenge of applying the human rights framework to the digital environment. The fact that such a wide range of stakeholders use and depend on ICTs for different reasons, coupled with the complex interaction between technology, politics and economics across the "layers" of digital environments, can make it difficult for policy makers to balance between rights and social goods. The report calls on the human rights community to provide guidance on the issues, and on policy makers to apply human rights values and principles to policy decisions. Policy should always aim to protect the open and empowering dimensions of digital environments.

The second cross cutting issue is the trend of governments placing increasing liability on intermediary service providers operating in digital environments. Whilst businesses do have responsibilities to respect human rights, placing excessive liability on companies that simply host content online or facilitate communication can have chilling effects on expression and innovation. Governments, companies, civil society and internet users should work together to find appropriate solutions.

Subsequent sections of the report examine four broad sets of opportunities and challenges that ICTs present for human rights.

**Freedom of expression censorship and control**

Opportunities and challenges relating to the rights to freedom of expression and association are explored in Chapter 2. The internet is increasing the ability of individuals to seek, receive and impart information and to collaborate with each other. Mobile phones are enhancing these capacities, allowing people to communicate with anyone, anywhere at any time. However, these new opportunities for freedom of expression and association are being eroded by a number of negative trends. These include the use of increasingly sophisticated and hidden censorship tools, and the use of the internet by human rights enemies and criminals for hate speech, child pornography and terrorism.

This chapter stresses the importance of achieving the correct balance between individual rights, and between these rights and the wider public interest, in online environments. It argues that any limitations placed on human rights online must be strictly proportionate, defined in law and necessary within a democratic society. Too often these strict principles, enshrined in international law, are ignored. The EU needs to lead by example, ensuring that its internal attempts to control hate speech and child pornography online do not provide a smokescreen for repressive states to censor legitimate speech.

The chapter also introduces the complexities involved in defining the roles and responsibilities of corporate actors to respect and protect human rights. It argues that the EU has an important role to play.
in positively supporting the corporate sector to behave in ways that respect and expand human rights. Top down legislation is not likely to be the most effective way to promote corporate social responsibility whilst also protecting the empowering and innovative characteristics of digital communications environments.

**Privacy, security and surveillance**

Chapter 3 explores opportunities and challenges relating to the right to privacy. Governments and businesses across the world are using ICTs to monitor the behaviour of citizens in increasingly sophisticated and hidden ways. Digital communications make it easier to collect, manipulate and share information about user activities and profiles. Business models are increasingly based around data mining practices in the search to maximise advertising revenue, consumer relevance and market share. Enhanced surveillance by governments has been spurred on by the so-called “war on terror” and the pursuit of public security. As a result, people are effectively losing the power to decide who has access to their personal data and what it is being used for.

In order to ensure that digital communications can support human rights as they continue to evolve, it is paramount that attempts to monitor and control communication in the name of security or consumer interest are strictly proportionate and maintain the careful balance between rights and social goods that is enshrined in the international human rights framework. Unfortunately, current practice does not achieve this, and urgent steps need to be taken by the EU to ensure that balance is restored.

**Access to knowledge, culture and ideas**

Chapter 4 concerns the right of people to take part in cultural life, to benefit from scientific progress and to access knowledge and information. Digital communications have unleashed tremendous new opportunities for creating, accessing and sharing knowledge in the public domain. This in turn enhances prospects for human empowerment and development. However, established gatekeepers and power holders feel threatened by the free flow of information and ideas that the internet facilitates. The result has been increased protection of copyright to unprecedented levels. This threatens to undermine individual rights to access knowledge and participate in cultural life, benefiting big business rather than human rights.

On balance, the EU has not played a positive role in supporting human rights within this policy sphere. Immediate remedial action needs to be taken, for example within ongoing negotiation on the multilateral Anti-Counterfeiting Trade Agreement. Rather than simply supporting dominant players within the creative industries, positive alternatives should that mutually support creators’ rights, innovation and trade should be given serious consideration.

**Pursuing development and equality in and through digital communications**

The fourth main set of opportunities and challenges relate to the broad umbrella right to development, discussed in Chapters 5 and 6. ICTs provide new tools for individuals and governments to improve access to income, employment, public services and overall economic development. Through enhancing information and communication flows, they also have an indirect empowering effect. However, the persistence of digital divides in access to ICTs and capacities to use them mean that these new opportunities are not accessible to all. This is particularly true of minority groups, poor communities and people with disabilities. There is also a significant gender divide in capacities to use and participate in
the governance of ICTs. These divides serve to reproduce and exacerbate structural inequality and discrimination. Proactive steps to enhance equality in and through digital communications are needed.

**Conclusions and recommendations**

As a powerful actor on the world stage and global region with the strongest human rights system, the EU has an important role to play in actively ensuring that digital communications environments at local and international levels support and expand human rights. Chapter 7 of the report identifies four main ways in which this should be done.

Firstly, the EU can influence international standards and practice indirectly through its internal policy, leading by example through ensuring that human rights within Europe are upheld, advanced and properly balanced within all policy that impacts upon communications. Secondly, the EU can influence international standards and practice directly through advancing progressive policy in international fora such as the Internet Governance Forum, the World Trade Organisation and the World Intellectual Property Organisation, and through bilateral and multilateral cooperation in policy spheres such as trade, copyright and development. Thirdly, it can use foreign diplomacy to encourage or pressure countries and institutions to uphold human rights. Fourthly, it can support companies and other stakeholders within its jurisdiction to build progressive business models and online practices that uphold and expand human rights.

Rather than following these policy approaches to build a positive policy framework, the report finds that policy makers have on the whole have tended to emphasise the negative dimensions of digital communications over the positive new opportunities that they present. As a result, there is an overarching trend towards taking measures to clamp down on the openness of communications environments, a trend which threatens to undermine their empowering nature and prospects for enhancing human rights. The challenge for the human rights community is therefore to find ways to maximise opportunities for harnessing ICTs to enable, promote and protect the realisation of human rights, whilst at the same time mitigating new challenges that threaten to undermine these efforts.

Particular care needs to be taken not to undermine the openness of digital environments inadvertently, for example through imposing excessive legal liability on intermediaries that simply facilitate online communication. This is because the empowering characteristics of digital communications stem from their openness, which in turn facilitates people-driven innovation, creativity and collaboration.

The report concludes that the EU should take the lead in building a positive and enabling policy framework to encourage digital communications to evolve in such a way as to support and expand human rights and the public interest. Communications are converging around internet-based networks, and the internet is central in nearly all policy areas and aspects of daily life. The EU’s policy framework therefore needs to be developed and applied in a consistent manner across a range of policy areas and across all “layers” of communications environments.
In Chapter 8, the report presents a number of recommendations and steps that the EU should take to support and expand human rights in the digital world. These are grouped under four main headings:

1. **Creative and coherent diplomacy and standard setting**
   - Digital communications concerns should be prominent in bilateral dialogues on human rights.
   - Respect for human rights online should be pursued within trade negotiations.
   - Rights-based policy should be promoted in and through the UN and other multilateral institutions, across all policy spheres, including those relating both indirectly and directly to internet governance.

2. **Promoting awareness and understanding of the issues**
   - Independent research should be commissioned to find solutions to complex problems and to ensure that policy is firmly rooted in evidence.
   - Dialogue should be promoted between different actors to promote learning and collaboration.
   - Public education should be undertaken to increase awareness and build the capacity of citizens to navigate around the issues and respect human rights.

3. **Fostering multi-stakeholder collaboration and problem solving**
   - Innovative and effective co-regulatory models should be developed and supported.
   - Partnerships between stakeholders to create tools to advance human rights online should be supported.
   - Multi-stakeholder governance and cooperation should be encouraged.

4. **Providing expertise and direct support**
   - An expert team on human rights and digital communications should be established within the EU’s External Action Service.
   - A resource centre for the deployment of ICT tools and solutions in emergency and humanitarian situations should be established.
   - Support should be provided directly to groups and networks that are defending human rights online.
   - Expanding communication access and capacities should be central within EU development cooperation.
INTRODUCTION

1.1 Setting the Scene

The purpose of this paper is to provide an overview of the main opportunities and challenges that digital networked communications present for human rights. It was commissioned by the European Parliament’s Enlarged Bureau of the Subcommittee on Human Rights (DROI) to support its debate on policy options in this field. The EU has an important role to play in developing policy and practice to enhance the opportunities and address the challenges that ICTs present for human rights. In order to do so, a thorough understanding of this landscape of challenges and opportunities is essential. This report provides the critical knowledge foundations for EU policy and activity in this increasingly important field of foreign and domestic affairs.

The explosion in access to digital communications over the last 20 years has been remarkable (see Figure 1). Whereas 15 years ago only 0.4% of the world’s population had access to the internet (see IDC cited in Internet World Statistics), by the end of 2009 an estimated 26% of the world’s population were using the internet, corresponding to 1.7 billion people (ITU, 2010:1). Internet usage is concentrated in the West, with internet penetration in developed countries estimated at 64%, as compared with 18% in developing countries (and only 14% if China is excluded) (ibid). However, almost all indicators suggest that this gap is diminishing (ibid:1-4). Notable trends include the use of mobile phones as a platform for internet access, with 1.2 billion people thought to access the internet using mobile browsers, compared with 1 billion people using PCs or laptops (UNESCO, 2009:46). There is also a trend towards increased use of fibre optic broadband which is helping to enhance the speed and quality of internet access. While this technology is the third most popular type of fixed broadband subscription, it has the greatest pace of expansion (ibid:54).

Increasing internet access both contributes to, and is driven by, advances in technology. Thus the last 15 years has seen a remarkable increase in computing processing power, together with new and improved tools (such as 3G phones and wireless networks) and applications (such as internet banking). These developments are set to continue, with projected improvements in terms of cost, power, functionality and usability. Likewise, the number of internet users is set to increase, with the National Science Foundation predicting that by 2020 there will be almost 5 billion internet users worldwide (cited in Network World, 2010).

The growth and development of digital communications is one of the most significant phenomena of the past two decades. In simple terms, the digitalisation of information -whether words, music or pictures - and the ability to access that information through a variety of devices, from the personal computer to the television to the mobile phone, have prompted a scale of change comparable to

---

1 This paper uses the term “ICTs” to refer to the most recent communications platforms that have emerged over the past century. Following Souter (2009a), these can be divided into four broad categories: computing and information technology; broadcasting, including radio and television; telecommunications via fixed and wireless networks; and the internet and internet-enabled services. This paper also uses the term “digital communications” which is slightly broader than “ICTs”, referring to not only communication tools and platforms, but also the products, services and applications that they support. “Communications environment” is used to describe the vast array of technologies, people, organisations and structures, and the interrelationships between them, that influence communication practices and activities. For further discussion of communications environments see Horner (2007a).
Gutenberg’s invention of the printing press (Myhrvold and Rinearson, 2003). People across the world are now increasingly able to access information, express themselves in the public domain, hold leaders to account and participate in economic, social and cultural activities that help to spur human development. However, ICTs have also unleashed new challenges and threats for human rights. Repressive governments and large corporations threaten to erode the new freedoms and opportunities that ICTs present for humankind through their attempts to maintain power and profit margins.

**Figure 1 - Changes in access to communications platforms, 1998-2009**

(Source: ITU, 2010).

### 1.2 The transformative and disruptive nature of digital communications

Communication is fundamental to human society. Indeed, it is impossible to conceive of human society existing without communication. From a human rights perspective there are three generally accepted reasons why communication is vital:

- It is a human need to be ourselves and have our own identity, and expressing ourselves through communication is how we experience our own humanity. In this sense, communication is essential to our human integrity.
- It is the foundation for other rights and freedoms. Without the ability to communicate it is impossible to realise or defend human rights, to have substantive democracy or to organise politically in any meaningful way.
- More recently economists such as Amartya Sen have argued that communication is a pre-condition for social and economic development.

In order to communicate with a wider range of people beyond face to face conversation, we need communication tools or platforms. For example, we can use a megaphone to amplify a human voice, and a cave painting or wall poster can be seen by many people even when the creator is not physically present. A newspaper, radio or TV transmitter reaches even further. All of these communication platforms - whether cave paintings, wall posters, books, print or broadcast - use a model of communication that we might call “one to many”. In this model there is a source of content production, such as a journalist, artist or publisher, whose content is then distributed to a wider audience. In the

---

2 See for example Dreze and Sen (1989)
past, the focus of human rights activity has been on the source of that content and the ability of that source to communicate free of censorship.

However, the growth of digital communication has changed this model dramatically. As the costs of connecting to the internet decrease across the world, the start-up costs for a digital media platform such as a blog similarly decrease. Content is being produced, shared, edited, re-edited and moderated by a growing community of online actors. This new model of communication can be described as “peer to peer”, in which the creation and sharing of content is distributed among many people who are simultaneously and directly communicating using digital platforms that can be accessed via a broad range of devices (such as the mobile phone computer, TV or radio).

"Peer to peer" networks have a number of characteristics that make them different to conventional "one to many" communication models. They are not controlled as easily, or in the same ways, as offline media, making both conventional censorship mechanisms and editorial standards hard to apply. The model facilitates the production of larger amounts of content, making us increasingly dependent on applications and intermediaries to arrange and curate that content, such as search engines and news portals. Users of digital communications have a much greater choice of content, and are able to impact on content production, presentation and modes of access much more than radio and newspaper audiences.

It is not that “one to many” models of communication are dying out, although increasingly some traditional media, such as newspapers in the most developed markets are finding a sustainable economic model increasingly difficult. Rather, they are being challenged and mutated by “peer to peer” forms of collaboration. The instantaneous nature of digital communications has made news cycles faster, placing media under pressure to foster continual communication with their audiences. Many media companies are becoming increasingly interactive, encouraging audiences to communicate with news producers through the use of mobile phones, cameras, texting, and email. People who were previously only consumers of news now want to be producers. Increasingly, user generated content that is published on social networking sites migrates to traditional media outlets, creating a continuous news cycle between citizens and media professionals (Beckett, 2008).

The right to expression has been in the hands of elites for much of human history, with writers, journalists, editors and publishers battling with governments and with each other over communication content and flows. The exhilarating prospect for the human rights movement is the potential to democratise freedom of expression itself, to wrest the platforms of communication from the hands of elites and place them in the hands of people. In order for this to happen, governments and regulators need to resist urges to control communication, be it in the name of promoting the public interest or in order to protect their power. It was the very openness of digital communication networks that enabled them to evolve into the powerful instruments and spaces for human rights that they are today. In our efforts to respond to the challenges and opportunities that ICTs present for human rights, care should be taken to protect the empowering and enabling characteristics of digital environments.

---

3 Between 2008 and 2009 the cost of ICT services dropped in all of the 161 countries included in the International Telecommunication Union’s analysis of affordability (ITU, 2010:5). Costs of mobile phone and internet services fell on average 15%. However, it should be noted that significant “digital divides” in access and affordability persist at international and local levels. On average, high speed internet connections cost 500% of the average monthly GNI per capita in Africa (ibid:8).
1.3 Opportunities and challenges for human rights: an overview of the issues

This report identifies four main sets of challenges and opportunities that digital communications present for human rights. The first of these relates to the rights to freedom of expression and association. ICTs are effectively democratizing expression, empowering people across the world to communicate directly with each other in the public sphere without having to go through communication gatekeepers such as the mainstream media. The internet is increasing the ability of individuals to seek, receive and impart information. Mobile phones are enhancing these capacities, allowing people to communicate with anyone, anywhere at any time. Digital communications have also transformed social activism through the use of websites, e-mails, social networking platforms and mobile phones in ways that would have been inconceivable even a few years previously. Barriers that previously restricted communication are being broken down. These include the need to have access to an expensive printing press, permission to use broadcast spectrum, and, with the spread of broadband internet, bandwidth limitations. Communications used to be slow and expensive. Now mobile phone and e-mail communications have dramatically reduced costs, and are rapidly developing almost ubiquitous reach.

However, these new opportunities for freedom of expression and association are being eroded by a number of negative trends. The first is the increasing use of ICTs to censor communications in ever more sophisticated and pervasive ways. The second is that many people fail to understand the responsibilities that come with the enhanced communication power granted by ICTs, leading to a flourishing of hate speech and misinformation on the internet. The third is that criminals are harnessing the power of digital communications to engage in activities that violate human rights, such as child pornography and terrorism. Whilst these threats are real and need to be taken seriously, policy makers have on the whole tended to emphasise the negative dimensions of digital communications over the positive new opportunities that they present. As a result, there is an overarching trend towards taking measures to clamp down on the openness of communications environments, a trend which threatens to undermine their empowering nature and prospects for enhancing human rights.

The second main set of opportunities and challenges relate to the right to privacy. In response to the potential for ICTs to be used by criminals, governments across the world are using ICTs to monitor the behaviour of citizens in increasingly sophisticated and hidden ways. This trend has been spurred on by the so-called “war on terror”. Digital communications make it easier for internet-based companies to collect, manipulate and share information about user activities and profiles. Business models are increasingly based around data mining practices in the search to maximise advertising revenue, consumer relevance and market share. Whilst this can benefit consumers, it also raises significant concerns for the human right to privacy. People are effectively losing the power to decide who has access to their personal data and what it is being used for.

The third main set of opportunities and challenges relate to the right of people to take part in cultural life, to benefit from the benefits of scientific progress and to access knowledge and information. Digital communications have unleashed tremendous new opportunities for creating, accessing and sharing knowledge in the public domain. This in turn enhances prospects for human empowerment and development. However, established gatekeepers and power holders feel threatened by the free flow of information and ideas that the internet facilitates. This is particularly true of large corporations whose business models depend on the protection of copyright. The human rights framework protects the rights of individuals to benefit from the moral and material interests that stem from their work and invention. However, this right is being abused by large corporations through increased and unwarranted protection of copyright that undermines individual rights to access knowledge and participate in cultural life to the benefit of big business rather than human rights.
The fourth main set of opportunities and challenges relate to the broad umbrella right to development. ICTs provide new tools for individuals and governments to improve access to income, employment, public services and overall economic development. Through enhancing information and communication flows, they also have a more indirect empowering effect, for example through making business more efficient. However, the persistence of digital divides in access to ICTs and capacities to use them mean that these new opportunities are not accessible to all. This is particularly true of minority groups, poor communities and people with disabilities. There is also a significant gender divide in capacities to use and participate in the governance of ICTs.

This report examines each of these sets of challenges and opportunities in turn, providing a broad overview of the issues that the EU should seek to address through its foreign policy. Each chapter examines the impacts that the evolution of ICTs has had on human rights, and discusses the ways in which domestic and external EU policy affects prospects for building national and global communications environments that protect and expand rights. Owing to the complexity of the subject matter and the broad range of human rights that are affected, it has not been possible to explore all of the issues in great depth or to provide concrete policy recommendations for each. Rather, the report provides insight into the nature of the challenges and opportunities at hand. It provides solid foundations for further research into specific issues, and the basis for policy development by the European Parliament, Commission and Council.

1.4 The “layer model” of digital communication environments: an analytical tool

The evolution of digital communications is not only presenting new opportunities and challenges for human rights, but is also changing the ways in which these opportunities and challenges need to be conceptualised and addressed. In the past, few human rights activists worried about the technology that delivered the content; they were largely concerned with the censorship of content. It did not matter so much what machines were used to create newsprint, or what type of cameras were used to film demonstrations. However, in the digital world, communications content and distribution is influenced more by the underlying technology, and often in ways that are hidden from the end-user. For example, equipment that provides network access can also be used to block access to sites for political reasons. Search engines that provide access to information can be programmed to exclude information that is unpalatable to the authorities. Mobile phone technology that is used to provide maps and navigation services can also be used by hostile governments to monitor and track citizens. Human rights advocates and defenders therefore need to think about applying human rights standards and values to the whole communication environment, rather than just to the content as they did previously.

In order to understand what this means in practice, it is useful to think of communications environments as being made up of a number of broad, overlapping conceptual “layers”:

- **Physical Infrastructure**: the basic cables, wireless towers and hardware that carry and route digital material.

---

4 Layer models are commonly used to depict communications structures, particularly in the telecommunications industry which uses a more technical model with more layers. This simplified layer model draws on Benkler (2000); Lessig (2001); Fransman (2001); and Mueller (1999). See Freedom of Expression Project (2008) for further discussion of this model and pertinent issues that need to be considered at each layer.
− **Connectivity**: the protocols and code that allow material to be transported across networks, and devices to receive and interpret digital data into the words, sounds and pictures that we understand.

− **Applications**: the platforms and tools that we use to create, view, manipulate and navigate digital content such as web browsers, search engines and blogging platforms.

− **Content**: the material that we are communicating - what we actually see, hear and watch.

These layers are illustrated in Figure 2. This illustration also shows that it is not just conventional policy makers – governments or public officials - who shape modern communications environments. They are also being driven by innovative businesses and, perhaps most radically, by everyday internet users themselves. These groups are influencing and changing the ways we communicate in unprecedented ways through online interactions and innovations which give rise to new communication tools, practices and norms. The digital world can best be thought of as growing and continually evolving ecosystem, rather than a centrally planned system with a goal or final configuration. It is a diverse, rapidly evolving, 'viral' communications space that is home to distinct communities with different needs and wants. It is shaped by what technology makes possible, by what users want and need, and by businesses aiming to fulfill these needs. Policy and activity is being shaped by markets, culture, norms and values as much as by regulators or governments, who often struggle to keep up with the rapid pace of change.

![Figure 2 - A layer model of digital networked communications](image-url)
Issues at each of the four layers of the digital communications model have significant implications for possibilities to protect and realise human rights. For example, at the infrastructure layer, the geographical reach of networks and hardware affects people’s ability to access and participate in digital communications. By the end of 2009 an estimated 18% of people in developing countries had access to the internet, compared to 64% in the more developed world (ITU, 2010). If people do not have access to ICTs, they are not able to enjoy the benefits that they offer. The types of hardware that are available also influence possibilities for enhancing human rights. For example, whilst mobile phones are becoming increasingly sophisticated and are helping to close digital divides between rich and poor, they are still not as flexible and powerful as personal computers.

At the connectivity layer, the internet initially developed as an open network over which anyone could send any form of digital data – words, music or images - using the universal code of Internet Protocol (IP). Increasingly governments are seeking to introduce controls at the connectivity level, and companies are seeking to shape internet traffic for commercial reasons. Such actions undermine the open ended “blindness” of the system to the data it carries, leaving content increasingly subject to censorship and control. While specific interest groups mobilise around issues such as network neutrality and open source technology, these tend to be technically-minded groups rather than the mainstream human rights movement.

At the applications layer, we are increasingly relying on intermediary companies and applications to help us to communicate across networks. These include search engines, social networking sites and platforms which host user generated content. As our reliance on these applications increases, so does their power to manipulate and control communication. Projects such as the Global Network Initiative have introduced a human rights dimension to debates concerning the responsibility that communication companies have when they are directly or indirectly being used by repressive states to control access to information. However, such initiatives remain low key, and are currently only supported by a relatively small number of human rights groups and communication companies.

At the content layer, the abundance of information and opinion online is challenging many traditional forms of authority. Whilst this is helping to democratise communication, it is also leading to a proliferation of uncivil speech and is leaving many unsure of what information to trust. While some human rights groups are active campaigners against censorship online, other issues at the content level remain outside the scope of the human rights movement. These include questions of intellectual property rights, inequality between the ability of different groups to create content, and how to tackle uncivil speech online.

Human rights standards and values thus need to be applied to all of the different layers within communication environments, and not just to the content layer as before. The EU could play a significant role in helping to develop a consistent policy framework to shape the totality of digital communications in a manner that supports human rights. This will require understanding not only of the convergence of communications around digital networks, but also of the increasing relevance of these networks in different policy spheres, including trade, intellectual property, media and development. A consistent policy approach is needed across these spheres that is aimed at fostering communications environments that are open, empowering and support the public interest.

1.5 Cross cutting issues

---

5 The Global Network Initiative brings companies, investors and civil society organisations together to produce principles and guidelines to help communications companies uphold human rights. See [http://www.globalnetworkinitiative.org/](http://www.globalnetworkinitiative.org/)
Two significant themes cut across the analysis contained in this report. The first relates to the importance of applying established human rights principles when balancing between human rights and social goods on the internet. The second relates to the trend of placing increasing legal liability on internet intermediaries, and the threats that this poses to maintaining open and empowering communication environments. These issues are briefly examined here in order to provide a backdrop for more in depth discussion in subsequent chapters of the report.

1.5.1 Balancing human rights on the internet

The international human rights framework carefully balances between the different rights and responsibilities that individuals have, and between the rights of individuals and the rights of the public or community in which they live. Human rights jurisprudence provides guidance on how to balance rights, and defines the limited circumstances in which rights can be restricted. However, technological, political, economic and social trends and dynamics within digital communications environments threaten to undermine the careful balance between rights that is mandated by human rights law. There is a need for the human rights community to take the lead in examining how the correct balance between human rights and social goods can be achieved in digital environments. The EU could play a leading role in ensuring that the correct balance is maintained and that human rights are upheld in communications policy and practice.

Within international treaties, restrictions are most commonly permitted to the rights to free expression, peaceful assembly, association, public media access to trials, appeal by aliens against expulsion and freedom of movement. However, international law is clear on the limited instances in which these qualified rights can be restricted. Article 19 of the ICCPR states that the right to freedom of expression can be limited as it “carries with it special duties and responsibilities”. However, restrictions are only permitted if they are provided for by law and necessary (a) to protect the rights or reputations of others and (b) for the protection of national security, public order, public health or morals.

Generally in international law, limitations to human rights have to meet a strict three part test. Firstly, limitations must be prescribed by law. This means that: (a) No limitation on the exercise of human rights can be made unless it is provided for by a law which is consistent with the Covenant and which is in force at the time the limitation is applied (i.e. it cannot be applied retrospectively). (b) Any such laws imposing limitations on the exercise of human rights shall not be arbitrary or unreasonable. (c) Legal rules limiting the exercise of human rights shall be clear and accessible to everyone. (d) Adequate safeguards and effective remedies shall be provided by law against illegal or abusive imposition or application of limitations on human rights.

Secondly, restrictions must be necessary in a democratic society. The burden of proof where a state imposes limitations is such that it must demonstrate that the limitations do not impair the democratic functioning of the society. While there is no single model of a democratic society, a society which recognises, respects and protects the human rights set forth in the Charter of the United Nations and the Universal Declaration of Human Rights is viewed as meeting this definition.

Finally, the limitation applied to the right must be proportionate to the nature of the risk that it is mitigating such as national security or public order. In other words, states cannot apply drastic limitations upon rights to meet a specific or limited threat, for example arresting or placing all members of a community under surveillance because of the deeds of a few.

The evolution of ICTs has brought with it new complexities in interpreting and applying these tests. Ensuring that limitations are prescribed by law is problematic as the internet is a transboundary medium that does not adhere to or respect national boundaries. What is prescribed by law in one country is not necessarily prescribed by law in other countries, yet the internet allows citizens to access
content that may be illegal in their own country but that is legal in the country in which it was uploaded.

The nature of internet communications makes it difficult to design measures to control information and activity online that are proportionate, narrowly targeted at the issue at hand and that do not unnecessarily undermine the rights and freedoms of others. Flows of information are in many ways more difficult to control online than offline. The international, networked structure of the internet and the ease with which digital content can be copied and distributed means that it is difficult both to track down and destroy unwanted material. For example, blanket measures to filter out illegal content inevitably also filter out legitimate content, and ongoing surveillance of internet users in the name of detecting criminal behaviour undermines the privacy rights of citizens.

It is also difficult to control online communication in such a way as to not impair the democratic functioning of society and undermine prospects for realising human rights. The internet is increasingly central to the everyday social, cultural, political and economic life of billions of people across the world. As this paper has illustrated, it has yielded numerous positive benefits for human kind, helping to strengthen democracy and human rights. Actions that undermine these benefits and threaten the continued evolution of the internet in the human interest should therefore be avoided.

The internet has arguably evolved into the powerful communication medium that it is today because it was originally designed to be open and free from regulatory control (Castells, 2001; Lessig, 2001; Benkler, 2006). The end-to-end principle was a key feature of this design, with adaptations, controls and intelligence being located at the edges of the network rather than embedded within it. This was so that any information could be transmitted across the network to any piece of hardware connected to it in a non-discriminatory manner using common protocols. A number of analysts have argued that we should be wary of meddling with these design principles through our attempts to control internet content as they may change the nature of the internet itself, inadvertently undermining the very characteristics that spurred its development (Benkler, 2006).

The challenge is to interpret and apply existing jurisprudence concerning the balancing of human rights in the light of current problems in digital environments. This should be done carefully and sensitively, ensuring that human rights are not violated, that the capacity of the internet to support human rights is not undermined, and that the rights and responsibilities of different stakeholders are clearly defined and understood by all. These issues are revisited throughout this report, mainly in relation to three instances in which it may be legitimate to put controls on internet content and activity: to preserve security, to restrict hate speech and to protect the rights of vulnerable groups, in particular children.

1.5.2 Intermediary Liability

A recurring theme that arises throughout this report is an identifiable trend of states increasingly imposing responsibilities and legal liability on internet intermediaries in an attempt to regulate online communication. The OECD (2010:10) has proposed the following definition of internet intermediaries:

“Internet intermediaries bring together or facilitate transactions between third parties on the Internet. They give access to, host, transmit and index content, products and services originated by third parties on the Internet or provide Internet-based services to third parties.”

The term encompasses a range of actors, services and platforms operating in digital environments including (OECD, 2010):

- Internet access and service providers (ISPs)
- Data processing and web hosting providers, including domain name registrars
− Internet search engines and portals
− E-commerce intermediaries and internet payment systems
− Participative networking platforms, including internet publishing and broadcasting platforms that do not themselves create or own the content being published or broadcast.

It is apparent from this list of actors and service providers that the internet and web would not have developed into what they are today without intermediaries. As well as providing social and economic benefits and value, they have been key in helping to enhance prospects for protecting and realising human rights through ICTs. For example, blog hosting platforms have enhanced individuals’ capacity to publish their opinions and analyses online and search engines help to improve access to knowledge through helping users to navigate around the Web. Many intermediaries in the applications layer enable creativity, collaboration and association, for example through public “collabowriting” tools such as wikis and through social networking sites. Others are essential for providing access to the internet such as ISPs, or helping to maintain the connectivity infrastructure and critical internet resources, such as domain name registrars.

Many of the private and public benefits that intermediaries provide stem from, or are enhanced by, their function as politically and socially "neutral" carriers of information. This neutrality has empowered internet users, allowing them to send and publish information that is accessible to anyone with an internet connection. In part because the internet developed historically as a medium relatively free from government regulation, and in part because of recognition of their important role in facilitating communication, expression and innovation, many countries have granted exemption for some intermediaries from liability for the communications content that they transport or host. It is generally recognised that liability for illegal content, such as hate speech or copyright infringing material, rests with the original sources of the information, and sometimes with the end user as in the case of child pornography in many countries. For example, the US Communications Decency Act (1996) states that, “no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another content provider” (cited in OECD, 2010:11). The European Electronic Commerce Directive (2000) exempts intermediaries from liability if they act as a “mere conduit” of information (ibid:12).

However, with rising concern amongst governments across the world to control online communication, the potential for intermediaries to become partners and vehicles for regulation has received increasing attention. For example, a number of countries are using hard and soft law to require ISPs to censor content in violation of freedom of expression, deny internet access to copyright violators and handover data about internet users in the name of protecting security.

This is a dangerous trend for three main reasons. Firstly, “neutral” intermediaries have played a key role in facilitating the growth of an open, collaborative and innovative internet. Imposing liability without careful consideration of the consequences threatens to change the very nature of the internet and undermine future potential for further positive innovation.

Secondly, imposing legal liability on services that host the communications content of other actors is likely to having a chilling effect on freedom of expression. Service providers and internet users are likely to be overzealous in their self-regulation in order to avoid breaking the law. The diversity of opinions, cultural content, political parody and pastiche expressed on platforms like YouTube will inevitably diminish if intermediaries restrict content and users self-censor.

Thirdly, methods through which internet intermediaries exercise control over communications content and user data are often opaque and not subject to public oversight. Many schemes that rely on ISPs to block access to illegal content depend on self-regulation by industry members who have little
understanding of what is legal and illegal, or of human rights. Many schemes violate the procedural rights of people they target, for example not providing access to a fair trial or right to appeal for users who feel that their rights to privacy or expression have been violated. The lack of public oversight also leaves the systems vulnerable to manipulation for political and economic reasons. Leaks of blacklists of sites that are blocked by some self-regulatory schemes have revealed restrictions on legal content. For example, a block list from Australia included online poker portals and sites containing information about euthanasia, pornography and religion (Brown, 2010). A Finnish list contained a site that criticised Finland’s blocking system (ibid). In short, as few schemes are designed with the human rights framework in mind, they tend not to contain substantive protections for freedom of expression, association or privacy (Brown, 2010; Rundle and Birdling, 2008).

Internet intermediaries have significant power within digital communications environments and play important roles in facilitating communication in private and public domains. This arguably confers certain social and moral responsibilities on them. Many intermediaries do engage in a degree of voluntary self-regulation, in some cases in an effort to avoid legislation and in others in response to growing public awareness about their potential role in human rights violations. For example, the world’s largest domain name registrar Go Daddy recently left the Chinese domain name market as it refused to comply with new directives from the country’s regulatory authority to collect further identification documentation from domain name registrants than had previously been required (Jones, 2010). Many online hosting service providers such as YouTube operate a “notice and takedown” policy for content that is identified by users as being illegal.

Whilst self-regulatory responses to illegal content can be problematic in terms of lacking protections for the procedural rights of accused parties, they help to maintain the openness of online communication that is vital for freedom of expression and communication in the public interest. However, there is much scope for designing better self-regulatory systems that uphold both the rights of individual users and the public interest. Such systems should be developed from the bottom-up, based on the needs and activities of internet users. They may be set up and facilitated by the state or by companies, but should be controlled and maintained by users themselves (Malhotra, 2007). In order to be in line with the International Covenant on Civil and Political Rights (ICCPR), the grounds and parameters (although not the mechanisms) for controlling online content should be clearly defined in law (Rundle and Birdling, 2008). All systems and procedures should be transparent, subject to public oversight and accountability, and uphold the procedural rights of internet users accused of violating the law.

There is a need for clarification about the roles and responsibilities that different stakeholders have for promoting human rights and public security in and through their activities in digital communications environments. This is particularly true for internet intermediaries whose position in digital environments lends them significant power, but whose political impartiality has helped to make the internet the innovative and useful communications medium that it is today. There is a particular need for these issues to be considered from a human rights perspective. International human rights bodies such as the European Court of Human Rights, the UN Human Rights Committee and the Committee for Economic, Social and Cultural Rights (CESCR) could help through providing guidance on applying human rights principles to address these contemporary challenges. Without strong participation from the human rights community in policy making and debate, there is a danger that the balance between human rights in the digital world will be tipped even further in favour of control rather than openness. This would severely damage prospects for harnessing ICTs to fully realise human rights.

1.6 The key message

The main argument put forwards by this report is that the EU needs to develop innovative approaches that respond to challenges in digital environments whilst at the same time maintaining their capacity to
support and advance human rights. This will require coordination across different policy spheres, from trade to development cooperation, in recognition of the indivisibility of both human rights and of converging communications environments. Owing to the transboundary nature of digital communication environments, it will require the harmonisation of domestic and international policy, with both working towards the goal of building open and liberating communications environments. To be successful, there is a need for fresh thinking and creative policy, based on bottom-up and collaborative partnerships aimed at empowering citizens, rather than top-down attempts to control communication.

2 FREEDOM OF EXPRESSION, CENSORSHIP AND CONTROL

This chapter discusses the impact that the evolution of ICTs is having on freedom of expression. It also considers the implications for other rights that are closely related to freedom of expression, in particular the rights to freedom of thought, free association and participation in government. The chapter begins with a brief outline of the importance of freedom of expression within the human rights framework and the significant new opportunities that digital communications are presenting for protecting and fully realising the right across all of its dimensions.

The chapter then moves on to examine challenges to freedom of expression online. It first considers how states around the world are increasingly censoring legitimate speech online, in violation of international human rights law. It uses case studies to describe the techniques which can be used to censor online communications, and provides an overview of why and how states are censoring for political, economic, social and cultural reasons. The role that Western businesses are playing in facilitating censorship is also discussed. The EU should work to provide companies with the positive support that they need to uphold human rights through their business models and practices.

The discussion then considers two instances in which human rights law permits restrictions to be placed on the free flow of information, namely for the regulation of hate speech and child pornography. Measures to control such illegal content online have largely been driven by moral panic, rather than by rigorous assessment of the extent of the risks at hand. As a result, insufficient attention has been paid to ensuring that controls are proportionate and do not place unnecessary restrictions on freedom of expression. Increasing burdens are also being placed on intermediary companies that facilitate the flow of information online. This negative policy making threatens to undermine the openness of the internet and its capacities to support innovation and information exchange.

The chapter stresses that human rights are indivisible, and that attempts to balance between rights online should follow the strict guidelines laid out within international human rights jurisprudence. The EU should lead by example in ensuring that its own internal policies are in line with the human rights framework. This would not only ensure that the rights of European citizens are upheld, but would also serve to raise global standards and avoid providing a smokescreen for censorship by repressive states. More support should also be given to private sector actors to help them respect and advance human rights through their business models and practice.

2.1 Freedom of expression as a foundation right

Freedom of expression is the right to hold and exchange opinions, ideas and information without impediment. Article 19 of the Universal Declaration of Human Rights (UDHR) states:

*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.*
Freedom of expression has long been regarded as a cornerstone human right, important both in itself and as an instrument to support other rights and democratic freedoms. For example, freedom of expression is essential for the realisation of the rights to freedom of thought and opinion (UDHR, Article 18), freedom of association (UDHR, Article 20), and participation in government (UDHR, Article 21). The instrumental nature of freedom of expression stems largely from the fact that the right encompasses both negative and positive dimensions. People not only have the right to receive information and ideas, but also the right to be able to seek and impart them. The exchange of opinions, ideas and information should therefore be capable of being a public act, not something confined to private discourse. This makes freedom of expression a strong foundation for democratic societies in which the rights of all individuals and communities are upheld.

The right to freedom of expression is not absolute. Human rights law state that in some cases it may be restricted to respect the “rights or reputations of others” (ICCPR, Art 19(3)(a)), or “for the protection of national security or of public order, or of public health or morals” (ibid (b)). Restrictions must be provided by law, necessary in a democratic society, and proportional to the legitimate aim.

The importance of the right to freedom of expression is reflected by its protection in all significant international and regional human rights treaties. These include: Article 19 of the International Covenant on Civil and Political Rights (ICCPR); Article 13 of the American Convention on Human Rights; Article 9 of the African Charter (elaborated by a specific declaration agreed in October 2002); and Article 11 of the European Convention on Human Rights (ECHR).

2.2 Democratising freedom of expression through digital communications

As discussed in the introduction, ICTs have expanded opportunities for both promoting and protecting freedom of expression across the three main dimensions defined in the UDHR, enhancing people’s ability to seek, receive and impart information. ICTs are providing people across the world with new communications tools and platforms, allowing them to engage with a wider range of people across longer distances at decreasing financial cost. This is true of communication in both the private and public spheres.

In the private domain, mobile phones and internet-based communication via email, online chat and voice-over-internet applications are making it easier for people to connect to each other for personal, business and political reasons. This has not only enhanced capacities to communicate, but also people’s ability to associate and organise with each other. Internet-based communications such as email listserv, information portals and social networking sites have made it easier for civil society organisations and networks of people interested in specific issues to communicate and coordinate with each other, sharing information, knowledge and experiences.

In the public domain, ICTs are also playing a significant role in enhancing expression and association. The ability of people to hold their leaders to account is a key tenet of liberal democracy, and depends largely on the nature and quality of public communication. In order to be accountable to citizens, states have to be able to understand and respond to their needs and opinions. The media have traditionally provided the main vehicles for communication between state and citizens, aggregating and reporting on public concerns and thereby helping to shape and express public opinion. The media also report on government policy and practice, with independent media playing a key role of scrutinising government through investigative journalism. The media have thus traditionally been powerful information and communication gatekeepers, with the content and nature of their reporting affecting the quality and nature of politics in countries across the world.

However, with the evolution of ICTs, people are no longer solely reliant on the mainstream media to impart and receive information in the public domain. The costs of publishing information have reduced
dramatically with the rise of the internet, which allows anyone with an internet connection to publish content via websites and blogs. People can now bypass the mainstream media entirely, getting news and opinion directly from their peers across the world rather than relying on third party reporting by journalists and media organisations. Navigation tools such as search engines and information portals help people to find the information that they are looking for online. The digitisation of literature, knowledge and cultural material is helping to break down physical barriers that in the past limited access to information, and translation tools are enhancing access to material published in different languages. A number of analysts have argued that public communication itself has been democratised, in turn enhancing public accountability and the free flow of information and ideas at local and global levels (Kaldor, 2008).

ICTs are also powerful tools for mobilising and campaigning, greatly enhancing the right to freedom of association and its positive impacts on democracy. For example, a number of studies have highlighted the significant role that SMS played in the 2001 mobilisation against, and eventual overthrow of, President Estrada of the Philippines following accusations of corruption (see for example Castells et al., 2007). More recent examples are discussed in section 2.3, including the use of ICTs for mobilisation and protest during the 2009 Iranian presidential election and the 2009 ethnic riots in Xinjiang, China. These cases also illustrate the ways in which ICTs are also greatly enhancing our ability to monitor human rights violations and to raise public awareness about them.

A number of characteristics of digital communications platforms make them more powerful tools for raising awareness about rights violations that the offline media. Firstly, many ICTs are networked, allowing users to communicate directly with other people who are connected to the network. For example, a photograph taken using a mobile phone can be directly transmitted across mobile phone networks to other phone users across the world. Phones connected to the internet can be used to upload photos onto the Web. A second, related point is that the increasingly networked nature of the global communications environment also makes communication harder to control. Images and information are easily replicated and shared, allowing multiple copies to be made extremely quickly and spread virally across communication networks. Thirdly, ICTs have increased the speed of information flows. Pictures can be transmitted across internet and mobile phone networks instantly, allowing people thousands of miles away to see events unfold in real time. Finally, ICTs are increasingly personal and mobile. Individuals carry personal mobile phones with them on a daily basis, giving them permanent access to communication networks that they can use immediately if and when the need arises. They also allow people to receive information directly from acquaintances that they know and trust, making them more powerful tools for mobilisation than information received via third party mass media (Castells et al., 2007).

2.3 The illegal censorship of legitimate speech online

Content is censored for a wide variety of reasons, some of which are legitimate under human rights law, the vast majority are not. This section is concerned with the illegal censorship of legitimate expression by repressive states. Instances in which it may be permissible to regulate speech are dealt with in subsequent parts of this chapter (child pornography and hate speech), and in the following chapter (public security).

2.3.1 Online censorship mechanisms
Whilst ICTs are helping to open up new spaces for private and public communication across the world, new tools for censorship and surveillance are also developing and spreading. The reasons why states engage in online censorship can be divided into four broad categories:

− **Political reasons** - the state censors content that contradicts its views and policies, threatens its authority, or is related to human rights.

− **Social & cultural reasons** - the state censors content that is deemed to be sensitive or offensive, such as that relating to sexuality, gambling, drugs and alcohol.

− **To promote security** - the state censors content that is believed to undermine national security or that threatens to provoke conflict, such as information about border disputes, separatist movements, and militant groups.

− **To restrict use of internet tools** - the state blocks or restricts access to applications and communication platforms hosted on the internet, such as email services, internet hosting, search engines, Voice over Internet Protocol (VoIP) services, and tools to circumvent censorship and surveillance.

A number of different tools and mechanisms are currently used by states to control the online activities of their citizens. This section is concerned with censorship that violates the right to freedom of expression. However, it should be noted that the tools described here are also used by states to control information flows for legitimate aims, such as to protect the human rights of others.

Censorship mechanisms can be divided into four main categories. Firstly, certain content or services online can be blocked or filtered so that users trying to access them are prevented from doing so. Blocking takes place at one or more of the gateways between the device through which the user is accessing the internet and the server upon which the information is being hosted. For example, software could be installed on users’ computers that blocks access to certain Web addresses, or internet service providers (ISPs) can be required to block access to the addresses of websites that contain certain key words. Common mechanisms used to filter content are outlined in Box 1.

### Box 1: Filtering Mechanisms

Filtering is the process of blocking an internet user from visiting certain websites. There are many different filtering mechanisms, and new ones are being developed all the time to tackle the latest circumvention tools. The most common technical filtering mechanisms are outlined below:

**DNS Tampering**: The DNS system matches domain names with the IP address that the mnemonic term corresponds with. This filtering mechanism involves blocking DNS servers from processing requests for IP addresses from a list of banned domain names.

**URL Filtering**: URLs are the full webpage names including the tool for retrieving it, such as [http://opennet.net/research/profiles/syria](http://opennet.net/research/profiles/syria). URL filtering can thus block specific web pages.

**IP Address Filtering**: Routers can be configured to drop packets which are destined for a banned IP address. It blocks all content using that IP address so can be very broad.

**Deep Packet Inspection (DPI)**: It is theoretically possible for systems to block websites based on analysing their content for banned topics.

**HTTP Proxy Filtering**: This technique forces/encourages all users to access web sites via a proxy server which prevents requests for banned sites from relaying.

---

6 This follows the Open Net Initiative’s categorisation of internet filtering practices. See ONI[b].
**Geolocation Filtering:** Websites can determine a user’s location by their IP address. This tool involves websites modifying or denying access to content depending on a user’s location.

**Content Filtering Software:** This is filtering software installed on an individual computer.

**Denial of Service attacks:** Whist this is not filtering, this technique produces the same end result. Websites or servers are overloaded with requests making them inaccessible.

These mechanisms require a list for blocking. Traditionally, lists are of banned websites and IP addresses. This can range from a specific webpage to much broader categories. For example, if blogspot.com is filtered it will prevent access to all the blogs hosted on that site, regardless of their content. In Syria, all access to the Israeli top level domain (.il) is blocked (ONI, 2009). Building a comprehensive list is difficult, particularly as content moves around and is saved in many places. Therefore, there are a growing number of countries using keyword lists. These lists block access to sites based on the words found in their URLs, or in their web searches. This tool is easy to administer but tends to block “innocuous as well as intended target sites” (Vitaliev, 2009:211).

**Sources:** ONI (2009) and Vitaliev (2009).

Secondly, content can be taken down from the internet. This can be achieved either through requesting that the internet service provider hosting offensive content removes it from their servers, or through disconnecting the servers that are hosting the content if they are located within the jurisdiction of the censoring government.

Thirdly, online content can effectively be hidden from users so that they do not know that it is available. This is most commonly done through preventing certain web pages from appearing in the results listed by internet search engines. One trend that has been identified in China is a move from ex-post towards ex-ante censorship. This involves the development of mechanisms to prevent "offensive" or illegal content from being published in the first place, for example with blog posts containing certain key words being held indefinitely in a moderation queue or being published in a “private view” that is never actually visible to the public (MacKinnon, 2009).

Finally, many states work to build a pervasive culture of self-censorship to prevent "unsuitable" content from being created or published online. In China, online activity is monitored both through automatic mechanisms and by internet police who actively "patrol" the web. The arrest and detention of high profile "cyber dissidents" can create a chilling effect, as can the dissemination of rules for online behaviour and penalties for breaking them. A number of countries, including China and Egypt, have taken steps to ensure that internet users are identifiable and traceable, limiting the scope for anonymous expression (ONI, 2009a; BBC News, 2010). Social techniques can also be employed, for example with CCTV cameras installed in internet cafes (Murdoch and Anderson, 2008).

These different censorship mechanisms are by no means mutually exclusive. States are increasingly using a number of different methods to both directly control access to content, and to stifle free speech online. The combination of methods used in the world’s most pervasive and sophisticated online censorship regime – China – is outlined in Box 2.

**Box 2: Censorship in China**

China has the largest and most sophisticated filtering system in the world, the so-called “great firewall of China”. The system uses a broad range of overlapping mechanisms to block access to content containing material considered politically sensitive by the authorities. Blocked materials cover a wide variety of topics including: Tibet, Falun Gong, Tiananmen Square, Taiwan independence, human rights, political reform, and critical or dissenting voices more generally.
A key strategy in the Chinese censorship system is to delegate responsibility to the private sector. In China companies and individuals are directly liable for content which appears on their website, even if that content is user-generated or details the results of a web search. However, the topics for censorship are not well defined, and thus the government can often ban material without having to lay out legal justifications. There is evidence that many demands for censorship are made during casual phone calls or instant messaging conversations. Likewise, companies are encouraged to over-censor materials to avoid the harsh punishments which include fines, licence revocation (and hence close of business) and criminal liability.

Another key tactic is to encourage self-censorship. Internet users in China are made to identify themselves at several stages, for example when registering a domain name or using a cybercafe. Online actions are also monitored through monitoring software on public computers, a physical cyber “army” or police force that patrols the web, and through collusion from the private sector. A good example of the latter is TomSkype, a joint venture between Skype and a local company. Whenever a user sends or receives a message containing a banned word, the conversation is saved together with the participants’ IP addresses, and this information is then made available to the authorities. The extent of user surveillance is not known, but when backed up with occasional high-profile detention, arrest and imprisonment of critical voices, the effect is increased self-censorship.

Other mechanisms used in the “great firewall” include using cyberattacks to block overseas websites at critical political moments (such as the sites of groups advocating human rights in Tibet in the run up to Olympic Games in August 2008), and, if all else fails, offsetting critical conversations through covert PR work. The Chinese authorities are said to have hired up to 280,000 people to steer online discussions in directions favourable to the establishment. These people are commonly known as the “Fifty Cent Party” which is allegedly their fee per comment that they post on the internet.

Source: MacKinnon (2010)

2.3.2 An International snapshot of censorship practices

Authoritarian and undemocratic states have always attempted to monitor and control communication and information flows through surveillance and censorship. However, the evolution of ICTs is shifting the nature of censorship, opening up new opportunities for control. Internet censorship is a rapidly growing trend, with RSF (2010) reporting a doubling in the number of countries experiencing online censorship since 2008 to 60 in 2009. The most significant trend is that censorship mechanisms are increasingly sophisticated and powerful, allowing censorship of online content to be more automated and systematic. Perhaps more dangerously, censorship mechanisms are increasingly invisible and are used to monitor communications without the knowledge of ICT users. Controls can be hidden in networks, protocols and software, and deployed by service providers that users trust such as search engines and content hosting platforms. When combined with ongoing surveillance and collection of data about users, these systems are not only powerful tools for controlling communication content and flows, but also for tracking down and controlling content creators themselves. Nearly 120 “cyberdissidents” were known to be in jail around the world in 2009, with the vast majority (72) in China (RSF, 2010).

Unsurprisingly, states that achieve low scores on indices of democracy and human rights are more likely to engage in internet censorship and surveillance of online activity. Research suggests that online censorship and surveillance is most pervasive in Burma, China, Iran, North Korea, Saudi Arabia, Syria, Tunisia, Uzbekistan and Vietnam (RSF, 2010). Online censorship is on the whole less common than censorship of the offline media, probably in part due to a lack of technical know-how and in part to lower volumes of content being available in local languages. It may also be related to relatively low
levels of internet access and technological development in a number of countries that have poor human rights protections. For example, there are few reported cases of internet censorship in sub-Saharan Africa, despite a number of countries in the continent having limited protections for human rights and civil liberties. Of a 2008 survey of four sub-Saharan African countries with limitations on press freedom, the Open Net Initiative found evidence of technical filtering in only one (Ethiopia) (ONI, 2008).

However, this trend is likely to reverse as internet access expands and more content becomes available in local languages. Draconian legislation to control online speech is emerging in many countries across the world. For example, in Belarus most independent newspapers have closed down, and there are no independent television or radio stations. This has made the internet a key source of non-state controlled information (AFP, 2010). As Andrei Bastunets, deputy chairman of the Belarusian Association of Journalists stated, “apart from the internet, Belarus practically has no free media” (ibid). In recognition of this, the attention of the Belarusian government is now turning to the internet. The government has made many attempts to interfere with free expression online, for example using cyber attacks against opposition websites and blocking the internet during major political events and demonstrations (RSF, 2010a). Earlier this year, in a move widely regarded as an effort to curb opposition activity in the run-up to the next presidential elections in 2011, President Lukashenko signed a Presidential Decree dramatically cutting down on the openness of the internet. This Decree on Measures to Improve the Use of the National Segment of the Internet Network requires ISPs and cyber cafes to identify and register all internet users, and information regarding connections are recorded and maintained for one year. The Decree also sets up an “Analysis Center” which is responsible for online surveillance and censorship reports to the President. The Analysis Centre assigns domain names and is empowered to order ISPs to close down websites. Ordinary citizens are also encouraged to request that websites are shut down (ibid).

At the global level, there is an emerging trend of increasing use of "just in time" blocking (Deibert and Rohozinski, 2010) or "tactical censorship" (Murdoch and Anderson, 2008) in which states introduce or enhance censorship during sensitive political periods. For example, during the 2007 protests against the Burmese Junta, the violent crackdown on protesters by the military corresponded with a communications crackdown. The regime took the drastic step of completely shutting down internet access in Burma. This was facilitated by the complete control that the junta has over the country’s internet gateways. That the regime took this step reveals the extent to which it felt threatened by the proliferation of unauthorized information sharing (Open Net Initiative, 2007). Similar cuts in internet access were reported during the 2009 presidential elections in Iran (Rahim, 2010) and the 2009 ethnic riots in Xinjiang, China (Reuters, 2009).

Internet access was also cut during the 2009 presidential elections in Iran. Following the elections in June, protests broke out across the country and internationally in support of the opposition candidate (Mir-Hossein Mousavi) and against alleged widespread electoral fraud. The internet proved a crucial platform for dissenters’ voices during the protests, allowing protesters to organise and rally support as well as to transmit information to the outside world. Footage of demonstrations captured on video-phones and posted on the internet proved particularly effective at galvanizing support for the protests. Twitter was used to transmit information about rallies and blow-by-blow accounts of action on the ground. Indeed, after foreign journalists were barred from attending “unauthorized demonstrations”, Twitter updates became an important news source for the Guardian, The New York Times and CNN, amongst others. Twitter’s role in the protests was judged so valuable that Twitter postponed a scheduled network upgrade (which would have disabled the service for some hours) following an appeal from the US State Department (Rahim, 2010).
The Iranian authorities responded with both physical violent crackdowns, and by seeking to control internet access. All internet access was cut off intermittently, access to some websites was denied and mobile phone services including SMS were blocked. Commentators noted that the internet had become “a virtual battle zone” (Rahim, 2010:8). In the aftermath, many of those arrested were reportedly beaten or tortured and subjected to show trials (European Parliament, 2010). The Iranian authorities have continued to interfere with freedom of expression, in particular by frequently jamming communication spaces including many international websites such as Facebook and Twitter.

Other significant global censorship trends include increased blocking of online tools and applications that could be used to access information and empower citizens, such as Google Earth in Morocco; blocking content published in local languages; and filtering at the edges of networks, for example through the installation of censorship software on computers. Analysts have also identified the emergence of "instream filtering" in which countries effectively share their filtering systems with neighbouring states (Zittrain and Palfrey, 2008).

2.3.3 The EU response

Online censorship is on the EU’s foreign policy agenda. In December 2009 the Council of the EU confirmed its “commitment to stepping up EU action on the relationship between freedom of expression and new technologies” (Council of the EU, 2010). The EU has responded by raising these issues in various forums including the UN Human Rights Council, the OSCE and the International Telecommunications Union. This has been achieved through speeches, resolutions and declarations which have both condemned the situations in a general sense, and have called for the authorities in these countries to act in accordance with established human rights standards (ibid).

For example, in March 2010, the European Council of Ministers issued a declaration condemning censorship in Iran. This highlighted the problems of jamming satellite broadcasts and filtering internet content during the recent elections, and called on the Iranian government to respect freedom of expression. The EU has gone further in some instances by looking at its relationship with individual countries and identifying specific areas where it might apply pressure. For example, Belarus is a member of the EU’s Easter Partnership, and the EU has repeatedly stated that it’s “readiness to further deepen relations with Belarus will depend on concrete steps in Belarus towards democracy, human rights and the rule of law” (Council of the EU 2010a). On an official visit to Belarus the Commissioner for External Relations and European Neighbourhood Policy gave a speech to Belarusian officials. In this speech the Commissioner reminded officials that positive action in the past had resulted in beneficial consequences. For example, the EU suspended the visa ban on certain political leaders following the release of political prisoners in 2008. He also suggested a range of benefits that the EU would offer to Belarus following satisfactory efforts progress on human rights protection. These included lighter visa requirements, closer trade relations and economic support (Ferrero-Waldner, 2009).

The European Parliament has adopted a number of resolutions, calling on the Commission and the Council to put pressure on countries to end censorship of the media and internet communications. These include have included Vietnam in 2008 (European Parliament, 2008a), and China and Iran in 2010 (European Parliament, 2010b and European Parliament, 2010c). In its resolution on Iran, Parliament connected a range of issues, such as Iran’s nuclear ambitions, with a range of politically motivated human rights violations, such as censorship and surveillance on the internet; arrest, detention and torture of dissidents; extra judicial killings; and the death penalty. The resolution reminds the Iranian authorities that political and economic relations with the EU (including trade agreements) are dependent on respect for human rights. However, direct calls to the Iranian government have proved fairly ineffective in the past, and therefore the resolution calls for numerous actions within the EU’s field
of competence, including debates on further targeted sanctions and support for initiatives aimed at improving media pluralism (European Parliament, 2010c).

These efforts are important, and Europe should continue to take a strong stance against censorship through diplomatic channels. However, online censorship tends to be included only in passing in EU declarations and resolutions, with little attention given to the range of mechanisms used and the pervasiveness of control across the different "layers" of communications environments. The internet tends to be treated as a subset of traditional media, rather than in its own right as a medium of human empowerment and development. Attention also tends to be focussed on the most notorious of the world's human rights violators. Little consideration is given to the increasing deployment of censorship mechanisms across the world, including in states that are seemingly politically benign, in increasingly subtle and hidden ways. Given that the internet spans national boundaries, protecting the openness of the internet in repressive countries is not only important for the citizens of those countries, but also for the continued development of a global internet that is open and empowering, rather than closed, fragmented and subject to control by repressive regimes. In short, there is scope for stronger and more consistent condemnation of internet censorship within the bilateral and multilateral diplomacy of the EU.

2.3.4 Roles and responsibilities of the corporate sector

The human rights framework has traditionally been concerned with mediating between states and citizens, ensuring that states protect, respect and fulfil the rights of their people. However, it is generally accepted that third parties also have responsibility to respect the rights of others, in particular businesses. The UN Human Rights Council has accepted a framework for addressing challenges posed by corporate entities to human rights. This framework emphasises not only the duty of the state to protect against human rights abuses by third parties, but also the responsibility of businesses to respect human rights (Resolution 8/7, cited in Ruggie, 2010). Communication companies therefore do have responsibilities to respect human rights, and it is also within their interests to do so in terms of maintaining a positive public profile.

There are numerous ways in which businesses can be complicit in censorship. States are increasingly using private intermediaries to implement or enhance censorship mechanisms. Many service providers and applications companies require licences to operate in certain countries, and these can be conditional upon adherence to specific requirements such as blocking access to certain kinds of content (Zittrain and Palfrey, 2008). This has been the case in China where many U.S. companies have been accused of providing direct support to the Chinese governments in its attempt to maintain a comprehensive censorship regime. In 2005 Yahoo assisted Chinese authorities in convicting four activists, including pro-democracy journalist Shi Tao, by handing over the contents of their emails, without asking what it was for (MacKinnon, 2010a). Microsoft has been accused of removing content before legally binding requests had been made and in an excessive manner. For instance, the company deleted the blog of a Chinese political blogger (Zhao Jing) following an informal request from a Chinese official (ibid). Google has also had a turbulent relationship with the Chinese authorities which recently culminated in Google pulling out of China (see Box 3).

In other cases technologies created by businesses is effectively pirated for use in censorship regimes. For example, in 2009 the Chinese government announced proposals to pre-install censorship software,
known as “Green Dam Youth Escort Programme” on all new computers. The US-based software firm Cybersitter has alleged that the code from its child protection software was stolen for use in the Green Dam scheme, and has filed a law suit in Los Angeles, naming the Chinese government, Chinese software firms and seven computer manufacturers (Guardian, 2010).

A further significant problem is that technologies that have been developed for legitimate purposes in one context can easily be used to violate human rights in other contexts (Zittrain and Palfrey, 2008). Hardware features designed to manage day-to-day internet traffic can be misused by repressive governments to censor traffic and monitor use. Some of the most sophisticated censorship systems have been designed using technology developed by Western companies. In many instances, the technology is sold directly to authoritarian regimes. In 2008, for instance, Nokia Siemens Network (NSN) sold communication monitoring equipment to the Iranian government as part of a larger contract to provide mobile phone technologies. The technology allegedly allowed Iranian authorities to use deep packet inspection (a technique whereby digitized information packets are deconstructed and examined for key words) to monitor online communications. Following the contested 2009 Iranian elections, internet speeds in Iran slowed drastically and some arrested activists allege that they were shown transcripts of their instant message conversations by authorities; these occurrences could suggest that deep packet inspection is being used. NSM argues that it provided the technology for the purpose of “lawful intercept” of information to track criminals and terrorists (Wall Street Journal, 2009).

There are thus various ways in which companies in democratic countries can assist with or contribute to illegal censorship and surveillance systems in other countries. In defence, companies often argue that they are enlarging the overall volume of information available in non-democratic countries, and that increased information will ultimately result in increased freedoms. Companies also argue that if they elect not to cooperate with non-democratic countries, the void will be filled with less scrupulous companies who may offer users even lower levels of internet freedom.

Box 3: Google in China

In 2006 Google entered the Chinese market, agreeing to censor search results according to Chinese law in order to obtain an operating license. Collusion in censorship did not sit easily with Google’s official mantra: “don’t be evil.” In June 2006 a senior policy counsel at Google stated: “Filtering our search results clearly compromises our mission... [Nevertheless] our continued engagement with China is the best (perhaps only) way for Google to help bring the tremendous benefits of universal information access to all our users there” (McLaughlin, 2006). Google’s compromise was to alert users to the fact that certain results had been blocked, and to store search records outside the country to ensure they could not be accessed by the government without the company’s consent. Studies often found that search results returned by Google were less censored than those delivered by Baidu, the market leader of search engines in China (Congressional Research Service, 2010, 7).

Over the past few years, however, censorship has not decreased in China; in fact, reports suggest it has expanded (MacKinnon, 2010, 2). In 2009 China publicly named and shamed Google for failing to prevent access to “undesirable” content and called for increased censorship (TechDirt, 2009). Concern mounted at Google and the situation came to a head when they discovered “a highly sophisticated and targeted attack on [their] corporate infrastructure originating from China” in December 2009.

7 The scheme has now been postponed, but it is unclear whether this was due to local and international outcry against the proposals or to legal issues and the need to allow manufacturers time to prepare. See Telegraph (2009a).
Information and Communication Technologies and Human Rights

(Drummond, 2010). Evidence suggested that the goal of the attacks was to access Gmail accounts belonging to Chinese human rights activists.

The worsening of the censorship climate, highlighted by the cyberattack led Google to "review the feasibility" of its Chinese operations. Following representations from the Chinese authorities that "self-censorship is a non-negotiable legal requirement" (Drummond, 2010a), Google decided to stop censoring search results, a decision which came into effect on March 22, 2010. Users accessing google.cn are now redirected to Google’s uncensored Hong Kong service.

On March 22 a Google search in China for “June 4” (the day of the 1989 Tiananmen Square massacre) returned 226 million results, where previously it had returned nothing (Singel, 2010). By March 25, however, users from mainland China using the Hong Kong site to search for sensitive information were no longer receiving access to uncensored results. Instead, searches usually returned “page cannot be displayed” error messages. The Chinese government had found a way of censoring the site (Wong and Marquez, 2010).

While many commentators applaud Google’s principled actions, others are concerned that Chinese people are now more reliant on Baidu, a more heavily censored search engine (Singel, 2010). So how can a business be ethical in this context? The answer is not simply about whether a company operates in a market, it’s also a question of how they operate there (MacKinnon, 2010b).

In 2006 the European Parliament adopted a resolution on Freedom of expression on the internet (European Parliament, 2006). This calls on the Council and the Commission to promote freedom of expression on the internet through its foreign relations, and to draw up a code of conduct that would limit the activities of companies operating in countries with limited human rights protections. Some MEPs have gone further, calling for a European version of the proposed US Global Online Freedom Act (GOFA) which would prevent US companies from assisting in censorship and repression in other countries (ALDE, 2007).

However, a number of analysts believe that legislation is too blunt an instrument to deal with the issues at hand (see for example Palfrey, 2008). Whilst civil liberties groups have supported the goals of GOFA in the USA, they have criticised certain provisions it contains as being unworkable. These include proposals to require companies to keep the personal data of internet users out of repressive countries at all times. This would be difficult given the necessity of using at least some data such as IP addresses to provide services, and the lack of a common definition concerning jurisdiction over companies operating on the internet (CDT, 2008). EU Commissioner Reding has opined that such a law in Europe would be too restrictive, placing companies in the difficult position of choosing between breaking the law and leaving “the market open to more unscrupulous operators” (Reuters, 2009b).

In response to these issues, the Global Network Initiative (GNI) ⁸ has attempted to provide realistic guidelines and best practice standards for companies when operating in countries with limited human rights protections. The GNI is a collaborative effort between companies, civil society and social investors to protect and advance freedom of expression and privacy in the ICT sector. The project was initiated in the USA, but is currently working to expand its reach and membership across the world. Corporate members of the GNI are required to “avoid or minimise the impact of government restrictions on freedom of expression”, protect the personal information of users in all countries they operate in, and uphold privacy rights when faced with demands from governments that are inconsistent with international privacy laws and standards (GNI Principles).

⁸ See http://www.globalnetworkinitiative.org/index.php
GNI guidelines outline a number of ways in which companies can minimise impact on freedom of expression when requested to restrict access to content. These include: requiring governments to abide by domestic law; interpreting demands narrowly; interpreting the government’s jurisdiction narrowly; and ensuring that users are aware how information is being censored (GNI Guidelines). Companies can also take procedural steps to bring their business models and operations in line with human rights. For example GNI Guidelines state that companies should develop internal procedures and structures to ensure that human rights are upheld throughout their operations, and should conduct rigorous human rights impact assessments and risk mitigation strategies.

There are signs that the initiative’s three corporate members are taking their commitments seriously, for example with Yahoo! establishing a Business and Human Rights Program and Google recently taking the decision to withdraw from China following attacks on its corporate infrastructure which were traced to the country (see Box 3). We recommend that the EU explores how it can support such co-regulatory initiatives such as the GNI in order to help companies uphold human rights through their business whilst at the same time encouraging the continued development of digital environments that are innovative and creative.

2.4 Legitimate regulation of speech online

The focus of the discussion so far has been on censorship by repressive states that is not acceptable under international human rights law. Attention now turns to two instances in which the human rights framework permits limitations to be placed on freedom of expression and the free flow of information: to protect children’s rights and to regulate hate speech.

2.4.1 Balancing civil rights with children’s rights online

Under the UN Convention on the Rights of the Child, children have a right to be protected from exploitation and the right to live and develop in a safe environment (Powell et al, 2010; Carr and Hilton, 2009). This has led to widespread efforts to protect children from exploitation in the online environment. Carr and Hilton (2009:15-16) group concerns about the risks that the internet presents to children into the following broad categories:

- Content: exposing children to illegal material (e.g. child pornography) or age-inappropriate content (e.g. adult pornography).
- Contact: exposing children to contact with sexual predators or harmful communities such as political extremists.
- Conduct: facilitating risky sexual interaction between children, sharing of personal information in the public domain and bullying.
- Commerce: providing access to age-inappropriate goods and services, and enhancing vulnerability to scams and fraud.
- Addiction: encouraging obsessive behaviour.
- Societal: creating a digital divide between children and compounding existing vulnerability of particular children.

Individual and state responses to these issues vary between households and countries. The most commonly employed means of restricting children’s access to inappropriate online material is the blocking or filtering of online content. This can happen at a number of levels, from installing software on personal computers through to ISPs blocking certain content or even embedding controls in backbone networks (Powell et al., 2010). Approaches to addressing other concerns vary according to the nature of the risk, for example with a number of social networking sites encouraging users to report suspicious behaviour to site administrators or to the police via buttons embedded on the sites.
Protecting the rights of children in the digital environment is essential. However, a number of human rights and digital liberties advocates have argued that the steps that are being taken in many countries are not only eroding the rights of adults to freedom of expression and privacy online, but also the rights of children to these freedoms. Powell et al. (2010) highlight how much of the popular discourse on these issues has been framed by a sense of fear and moral panic about the effects that ICTs are having on society, exacerbated by emotional appeals for child protection and security. Public policy and the implementation of systems to protect children have largely been driven by this moral panic, rather than by informed discussion about balancing the rights of different stakeholders and by evidence relating to the nature and extent of the risks involved. As a result, freedom of expression and privacy advocates have tended to be presented as being diametrically opposed to children’s rights advocates. The differences in opinion between the two groups have tended to be exaggerated, with little attention paid to the indivisibility of human rights and the complementarities and overlaps between children’s rights and civil and political rights.

Civil liberties and children’s rights advocates have been critical of the European Commission’s proposals for a Directive on combating sexual abuse, sexual exploitation of children and child pornography, adopted in March 2010 (McNamee, 2010; EDRI, 2010a). Of particular concern are proposals to block websites concerning child pornography. Blocking can be circumvented, presents a danger that access to legitimate sites will be mistakenly restricted and fails to address the root cause of the problem. These measures are therefore likely to be ineffective in protecting children, and threaten to place disproportionate and unnecessary restrictions on the free flow of legitimate information and ideas. They also set a dangerous precedent in terms of sending the message to the international community that blocking is acceptable practice, providing repressive regimes with smokescreens behind which to censor legitimate expression online. The EU is obliged to protect children’s rights online, but greater attention needs to be paid to ensuring that measures do not place unnecessary restrictions on the civil rights of adults or children, and that they do not unnecessarily undermine the openness of digital communications environments at national, regional and international levels.

Polarisation of the debate into “children’s rights versus civil liberties” is concerning for a number of reasons. Firstly, it presents the danger that inappropriate approaches are taken, driven by popular and politicised arguments rather than informed debate and analysis. Secondly, it exacerbates the danger of children’s rights being used as a smokescreen to control online behaviour in illegitimate ways. Powell et al. (2010) highlight how child protection legislation has often been hijacked by groups seeking to protect other interests, such as the fight against internet fraud and copyright violation. Moreover, if countries with relatively good records of human rights protection implement well-intentioned but ill-informed measures to protect children online, there is a danger that such measures will start to informally set international standards. The implications of this are all the more severe in countries with limited human rights protections, with democratic countries effectively exporting bad practice that allows authoritarian countries to violate human rights in the name of child protection.

In 2009, the Oxford Internet Institute held an event to address these issues, convening a discussion between child rights and civil liberties groups. The resulting policy discussion paper stresses that there are in reality more points of agreement between the two constituencies than is often believed to be the case, and argues that policy processes should build upon these areas of consensus in order to effectively balance the rights of all stakeholders online (Powell et al., 2010). The paper suggests that seeds of agreement are starting to grow in the following areas:

− All stakeholders would benefit from a safer internet environment. This would result in less pressure to limit expression and erode privacy rights online.
Policy responses and practical approaches to the issues should be rooted in rigorous research and thorough understanding of the issues at hand. Recent research suggests that the risks that children face online are not very different to those faced offline, and that the experience of risk is different for individual children. For example, children engaging in risky behaviour offline are more likely to engage in it online, and experiences of risk vary with factors such as the psychological makeup of children and dynamics within their family or home (Palfrey et al., 2009; Livingstone, 2007).

The implication of this research is that policy responses should be clear, specific and targeted at the most significant risks. Blanket measures are likely to be inappropriate. Palliative solutions should be accompanied by preventative approaches, with effort focused on preventing activity that is harmful to children in the first place.

Blocking illegal content online is acceptable from a human rights perspective. Whilst there is significant disagreement about how this should be done, there is general agreement that measures should be transparent, targeted, specific, flexible and meet the specific needs and preferences of users.

### 2.4.2 Regulating hate speech

Hate speech can be defined as any form of expression that vilifies an individual or group on the basis of a certain characteristic such as race, religion, nationality, gender or sexual orientation. In many jurisdictions hate speech is prohibited on the grounds that it undermines the dignity of its victims and can incite violence or discriminatory action. This is provided for in Article 20(2) of the ICCPR which states that "Any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law".

Most European jurisdictions contain prohibitions against hate speech, although there are considerable variations between states. In the USA, the First Amendment of the Constitution prevents the regulation of the content of speech, subject to exceptions such as defamation and incitement to riot. This historic divide between the level of protection offered by hate speech in the US and elsewhere, in particular Europe, has led to considerable differences of interpretation of what constitutes legitimate and illegitimate expression on the transboundary medium of the internet.

The internet and related ICTs have arguably enhanced opportunities for hate speech and increased the threats that it poses to individuals and communities. It has been stated that the internet is “a relatively cheap and highly effective tool for racist individuals or groups to spread hateful ideas to an audience of thousands, if not millions” (Commission of the European Communities, 2001). However, there is some debate as to whether hate speech can and should be regulated online as it is in the traditional media. In the USA, the Supreme Court has taken the different characteristics of different types of media outlet into consideration when analysing whether restrictions are in line with the First Amendment. It has ruled that the internet “is entitled to the highest protection from governmental intrusion”, owing to its historical lack of regulation and the fact that it is not as intrusive as broadcast media or limited to control by a small number of stakeholders as in the case of traditional offline media (Timofeeva, 2003). In contrast, most states do not treat the internet as being different to other forms of media, for example with hate speech regulation, including the banning of Nazi propaganda, being enforced online as it is offline in Germany (ibid).

The transboundary nature of the internet makes it difficult to regulate hate speech online. There is little to prevent people from accessing material that is illegal in their country but that has been published and is hosted elsewhere. Governments can issue notices to ISPs based within their own jurisdiction to take down illegal content, but they have limited power over ISPs operating from other countries. The Additional Protocol to the Council of Europe Convention on Cybercrime was one response to this issue,
aiming to create common standards and approaches for party states. However its ability to regulate hate speech online will be limited given the reluctance of a number of states to sign up, including the USA.

A worrying development in the area of hate speech has been the concerted attempt, led by a number of Islamic countries, to expand the notion of hate speech to include "defamation of religions" (and in particular, Islam). Over the past 10 years, sympathy for these arguments has increased within UN institutions such as the Human Rights Council and even the General Assembly, perhaps in relation to the expansion of freedom of expression facilitated by digital communications. This is concerning. Extending legitimate limitations on freedom of expression to cover speech directed against a belief, rather than against an individual or group of individuals, will have a chilling effect on freedom of expression, and may be used by certain governments to justify suppression of dissent.

2.4.3 The roles and responsibilities of the corporate sector

A number of cases have illustrated that it is possible for states to control illegal content online through employing the same filtering and blocking techniques that are used in internet censorship. When seeking to regulate illegal content online, states should note that the approach and mechanisms selected can affect human rights in different ways. For example, filtering is not an exact science. Many freedom of expression advocates therefore call for illegal material to be deleted at source rather than filtered. This technique is more precise and minimizes the risks of innocuous material being removed. However deleting does require more resources than blocking, and can be difficult when content is hosted in other jurisdictions. Filtering is therefore often preferred to deletion within international policy as it is the easier option, despite it having damaging implications for human rights. However, in some instances, filtering may be desirable to deletion, in particular when targeted at content that is permitted by human rights law but that is deemed unacceptable by individual countries. In these cases, deleting material can have an overbroad effect as it infringes upon access to that content for everyone and not just those in a particular jurisdiction. Before implementing any mechanisms to control information online, states should undertake rigorous risk assessments of the likely impact on human rights and on the openness of the internet as a whole. Mechanisms selected must be strictly proportionate and affect only illegal content. Sadly, these factors are rarely taken into consideration in the design of systems to regulate online communication.

There is an increasing trend across the world of states holding ISPs and other intermediaries responsible for monitoring and controlling the online activities of their subscribers (Vitaliev, 2009). This is a dangerous trend which threatens to undermine the openness of the internet through placing responsibility for the public regulation of content in the hands of private companies which have little knowledge of human rights and which users trust and believe to be politically neutral. Requirements are often broad and vague, leading to more pervasive censorship as service providers strive to escape punitive measures from the state. Content carriers are incentivised to restrict the use of their services for engaging in online communication or other activities that might be deemed controversial, with a chilling effect on freedom of expression (GNI, 2009). Box 4 contains two examples of intermediary liability imposed in two European countries: France and Italy. Both concern expression which may lawfully be censored. However, in the first, steps were taken to try and limit the impact of the restrictions on access to content and the openness of communication outside of French jurisdiction. In the second, criminal liability has been placed on individual staff members of an online company that hosts user-generated content. This has set a dangerous legal precedent that, if upheld, would make companies increasingly wary of facilitating open and free communication between internet users online.
Box 4: Who is responsible for illegal content online?

Yahoo! and Nazi Memorabilia, France

In April 2000, a French citizen, acting through an NGO, initiated proceedings against the US company Yahoo! in a French court. The complainant had requested that Yahoo! remove Nazi memorabilia that was available on the US Yahoo! shopping website, accessible from Paris, but the company declined to oblige. Prosecutors alleged that Yahoo! was violating French laws which ban the trafficking of Nazi goods.

Yahoo! countered that it would be impossible for them to comply with this law due to the transboundary nature of the internet and the fact that selling such goods is not illegal in all countries across the world. They argued that deleting the content would radically change the nature of the internet as it would prompt restrictions according to the lowest common denominator. This would effectively mean that content deemed “undesirable” by repressive states would have to be eradicated from the web.

The court ruled that Yahoo! was obliged to take all necessary measures to dissuade French web surfers from accessing information illegal Nazi auction sites via Yahoo!. This was based on recommendations from internet experts who argued that Yahoo! could employ tools to determine the geographical location of customers and block content that is illegal within their jurisdiction.

Google and offensive content, Italy

In 2006 four school children in Turin, Italy made a short film of themselves bullying a class mate and uploaded it on Google Video (a user-generated video platform). Following a formal complaint from the police, Google removed the video within two hours (Sucherman, 2010). This was in line with the EU Electronic Commerce Directive which establishes exemption of liability for service providers when illegal materials are removed promptly following notice. However, Italian prosecutors initiated criminal proceedings against four Google executives on grounds of defamation and privacy violations. The prosecutors alleged that, as Google handles user data and uses it to generate advertising revenue, it is a content rather than a service provider.

In February 2010 the Court absolved all defendants for defamation. However, three of the employees were convicted in absentia for privacy violations and were given suspended six-month jail sentences. The ruling is subject to appeal and Google has said it will vigorously take up this opportunity.

This ruling has been heavily criticised. It effectively mandates internet intermediaries to pre-screen user-generated content. This would be difficult given the vast volumes of content involved; Google claims that on average, 20 hours worth of video content is uploaded every minute. More importantly, the ruling places disproportionate responsibility on intermediaries to interpret the law. Were such rulings to become common, the effect would inevitably be to chill freedom of expression and undermine the capacity of the internet to be an empowering communications medium. The case was also unique in imposing criminal liability on individuals, rather than civil liability on the firm. The employees were seemingly selected by the prosecution at random; none of them live in Italy or have direct responsibility for the video in question (BBC News, 2010).

Similar cases are ongoing in Italy against other intermediaries including eBay, Yahoo and Facebook (BBC News, 2010).


2.5 Expanding the public interest dimensions of digital communications
Debates about controlling hate speech online are often mixed up with concerns about preserving access to quality, public interest content online. As already discussed, the evolution of digital communications has empowered citizens to participate directly in media environments, bypassing the traditional mass media to communicate directly with their peers via blogs, video and social networking sites. Whilst this is helping to enhance individuals’ ability to impart information, a number of commentators are concerned that it is threatening to undermine capacities to seek accurate information (see for example Carr, 2008). They argue that digital communications environments suffer from “information overload”, with internet users unable to distinguish between accurate information and falsehood, and with rationale public debate led by professional journalists collapsing into inclusive but heated and uninformed argument (Keen, 2007). Complaints that the internet has unleashed “too much freedom of expression” are common in policy debates across the world⁹.

These debates are resulting in ICTs being framed in an increasingly negative light within policy discussion. Solutions to problems that have arisen with the evolution of digital communications commonly focus on controlling and clamping down on online communication. This is dangerous from a human rights perspective as it threatens to erode the empowering communication spaces that ICTs have helped to open. Rather than attempting to control online communication, policy makers should be seeking to enhance the communications literacy of users, providing them with the skills and capacities that they need to navigate new and emerging communications spaces. Similarly, instead of attempting to make all people communicating online conform to professional journalistic standards, professional investigative media should be supported. Evidence suggests that media audiences still on the whole trust news and information from traditional media brands more than alternative sources (Pew, 2009; Reuters, 2009a). It therefore makes sense to support information gatekeepers that act in the public interest, rather than clamp down on those who may not; there is still a space for publically owned, public interest media and communications in the digital age.

At the applications “layer” of digital environments, the roles and responsibilities of search engines is another popular subject of discussion within communication policy debate. As a result of the vast amount of information that is available online, users are increasingly relying on search engines to find and access the information that they need. Most of the business models of the world’s most popular search engines rely on advertising revenue. Whilst search engines rely on increasing market share through providing useful search results, this does not necessarily equate to providing access to information that is accurate and that helps to foster healthy democratic debate. Research suggests that 97% of internet users rarely look beyond the first three search results (Avtec, 2006), and in 2005 only 38% of internet users in the USA were aware of the difference between links that are sponsored by companies and those that are not (Pew, 2005).

As argued throughout this report, the emergence of new, open communication spaces in the digital environment has yielded too many opportunities for the advancement of human rights to risk undermining them through placing excessive controls on the platforms and facilitators that we depend on for communication online. Innovative approaches need to be found that preserve open communication whilst at the same time fostering capacities and spaces for public interest communication that strengthen human rights and democracy. In the case of search engines, this might mean supporting public search tools and portals, rather than requiring private companies to prioritise access to certain forms of content.

---

⁹ This concern was voiced in Freedom of Expression Project workshops in Latin America, Africa, Asia and Europe. See http://www.freedomofexpression.org.uk
At the connectivity and code “layer” of communications environments, the issue of “network neutrality” has arisen within many national and international policy debates in recent years. The term refers to the original design of the internet as a “dumb” network which does not distinguish between the types or content of data sent across it. All data sent across the network would be treated equally. This design effectively helped to give all users the same powers of communication, regardless of their resources or social status. Concerns about network neutrality initially arose in the USA in response to proposals by some internet service providers to allow content companies to pay for the prioritisation of their data across networks.

Today’s internet is not neutral. For example, service providers can legitimately give priority to real-time visual and audio content in order to ensure that it maintains its integrity and quality as it travels between end users engaging in video conferencing or watching television over the internet. Such behaviour is commonly referred to as traffic shaping. Rather than being free from all traffic shaping and prioritisation techniques, there is emerging agreement amongst analysts that the internet should not be subject to arbitrary or purely political or profit-driven, anti-competitive discrimination of content. If it is strictly necessary, traffic shaping should be transparent, and is generally only acceptable to maintain quality of service that benefits end users. To preserve the openness and versatility of networks, traffic shaping and content controls should not be embedded within networks themselves.

2.6 Conclusions

This chapter has shown how digital communications have opened up tremendous new opportunities for realising the right to freedom of expression. They are helping to empower people to express themselves directly in public arenas without having to go through traditional media gatekeepers. They are also providing new means to seek and receive information, as well as greatly increasing the amount of information, knowledge and cultural material that can be accessed. In opening up these opportunities, digital communications are also helping to more fully realise other human rights, such as those to freedom of association and participation in government.

As a proponent of freedom of expression on the international stage, the EU has a significant role to play in ensuring that these new opportunities presented by ICTs remain open at national and international levels. The EU should also be seeking to expand opportunities for the further development of technologies to fight rights violations, to increase accountability and to allow people to express themselves politically, culturally and socially. This will require an overarching policy of maintaining open and innovative digital communications environments to counteract the increasing trend of governments to seek to clamp down and control online communication, both in democratic and repressive states. This policy could be implemented on a number of levels.

Firstly, the EU should promote respect for freedom of expression within its bilateral and multilateral relations and negotiations. This is already EU policy, but there is scope for more explicit and consistent advocacy for the protection of human rights online. Secondly, work could be done to raise awareness and capacity amongst human rights defenders of the potential for using digital communications, and about how to circumnavigate dangers that may be hidden at the different layers within communication networks in terms of censorship and surveillance.

Thirdly, the EU should actively participate in policy dialogue at national, regional and global levels to promote a culture of open communications rather than cultures of control. Innovative solutions to problems should be encouraged that place emphasis on expanding the positive dimensions of ICTs rather than on controlling negative practice that they support. These could be based on promoting the expansion of public interest communication spaces. Building public understanding about the nature of digital environments (i.e. communications literacy) is equally important in order to empower users to
participate fully and responsibly within them. Businesses should also be supported to operate responsibly in ways that protect and promote human rights, whilst at the same time encouraging innovation and business development.

Finally, the EU should ensure that its domestic policy does not directly or indirectly lead to the development of international norms that threaten freedom of expression. Similarly, in seeking to control damaging speech and behaviour online, it should take care not to export bad practice or to provide a smokescreen behind which legitimate expression is controlled in repressive states in the name of protecting security or child safety.

3 PRIVACY, SECURITY AND SURVEILLANCE: THE NEED FOR BALANCE

This chapter examines the ways in which the evolution of ICTs is impacting on the right to privacy. Technologies can help to enhance personal privacy, for example through allowing us to communicate anonymously in online spaces and encrypt information that we send across communication networks. However, the main concerns that privacy advocates have in the arena of digital communications relate to the dangers rather than the opportunities that they pose to privacy rights. This chapter outlines these challenges.

The chapter begins with an examination of the role of the right to privacy within the international human rights framework, stressing its importance for supporting other rights such as freedom of expression. Next, the chapter describes the ways in which ICTs are making it easier for states and businesses to violate privacy rights, for example through making it easier to collect and analyse increasing volumes of personal information.

The chapter then moves on to consider two main policy areas which concern privacy advocates: the manipulation of personal data for commercial purposes, and increasing surveillance of citizens by states in the name of enhancing public security. Owing to the growing centrality of the internet in daily life, it is increasingly easy for companies and governments to build up accurate profiles of people’s personalities, preferences and activities through examining data trails that they leave behind them online. The business models of many companies depend on these profiles as they allow them to tailor services to the needs and preferences of individuals, and to target advertising better. Whilst this can help benefit consumers, internet users are increasingly unable to control who has access to their personal data. They are also unable to control the collection and use of their data by states in their attempts to track down criminals and restrict the use of the internet for criminal purposes.

In the commercial arena, progress is being made to advance privacy rights through data protection regulation in Europe. However, there is still work to be done at the international level in raising and harmonising standards. In the arena of public security, policy and regulatory approaches that are being taken at EU and global levels have not achieved the balance between public security and individual rights that human rights law requires. Concerns about the use of digital communications for terrorism and other digital activity tend to be prioritised over concerns to protect privacy rights and expand the empowering dimensions of digital communication. This is overwhelmingly due to moral panic in the wake of the “war on terror”, rather than the result of rigorous research into the nature of the threats at hand and proportionate responses to them.

Protecting and promoting civil liberties will be essential for both economic development online, and for the success of the international battle against terrorism and extremism. This should be reflected in the internal and external policy of the EU and its member states, in trade, communications, security and human rights policy.
3.1 Privacy within the international human rights framework

Article 12 of the UDHR states that “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.” The language of Article 17 of the International Covenant on Civil and Political Rights (ICCPR) mimics that of the UDHR, with the addition that interferences with privacy must not be ‘unlawful’. Almost every country in the world explicitly or implicitly includes a right to privacy in its constitution (Privacy International, 2006).

The right to privacy is essential to human dignity and indeed to individuality; we are less able to be ourselves if all our actions are watched and catalogued. The right also has instrumental value, as democracy and liberty rely on individuals having a certain degree of privacy. The right to privacy underpins many human rights, including the right to freedom of association, freedom of belief and freedom of expression. As one writer puts it “in one sense, all human rights are aspects of the right to privacy” (Volio, 1981).

Whilst privacy is a fundamental right, it is not an absolute right. Defining the right to privacy requires a balancing between that right and others (e.g. freedom of expression), as well as a limited range of national or societal concerns. However, as with other qualified rights, the restrictions that can be placed on the right to privacy have been interpreted narrowly within international jurisprudence, and must be laid out in law, necessary and for a legitimate aim. For example, the European Court of Human Rights has imposed sanctions on numerous countries for failing to regulate surveillance measures (see e.g. Huvig v France), and has ruled that individuals should have access to their personal records (e.g. Gaskin v UK).

3.2 Challenges to privacy: enhanced surveillance and data collection

Whilst individuals’ privacy rights have been threatened by state and corporate activity throughout history, the evolution of ICTs has made the dangers far more pronounced. Digital communications have revolutionised society, but on the flip side have made the ability to monitor others easier, cheaper and more efficient. ICTs have enhanced threats to privacy in three main ways. Firstly, they are enabling the collection and storage of increasing volumes of personal information. Secondly, they are making the consolidation and analysis of this information easier and more efficient. Thirdly, they have made it increasingly difficult for people to protect their personal data and know who has access to it. This section explores each of these challenges in turn.

3.2.1 Enabling the collection and monitoring of increasing volumes of personal information

ICTs, and in particular the internet, are far more interactive compared to traditional offline media such as broadcast and radio. Users provide information about themselves through their interactions with the technology – what searches they make, what links they click on, what pages they look at and for how long. New technological tools and devices are often designed to collect this information, including the TiVo (a device that allows users to watch television over the internet), the gaming platform Xbox360 and the online literature platform Google Books (Privacy International, 2006). Furthermore, technology, and the internet in particular, is used increasingly in everyday interactions including banking, shopping, and socializing. The result is that people are giving away far more of their personal data and information about their habits and activities, including financial, health-related and sexuality information. Technology is thus allowing ever greater amounts of information to be gathered. As Lawrence Lessig points out, “your life becomes an ever-increasing record” (1999:152).

Each computer, mobile phone or other device that is used to access the internet has a unique IP address, which means that they can potentially be traced. IP addresses can be tied to a person’s physical...
identity in a number of ways. For example, many websites and ISPs have developed authentication systems which involve identity disclosure (particularly during electronic commercial transactions); governments may require internet users to register their IP addresses; and identity characteristics can be deduced through data mining and analysis of a person’s online actions (see below). For example, two students at MIT developed a software programme which allowed them to predict users’ sexuality through analysing their online connections to other people on a social networking site (Johnson, 2009). Such technology could have severe implications, for example if used in countries where homosexuality is illegal, or if adapted to detect other traits, such as a propensity to commit crime.

A number of tools have been developed to track the activities of internet users. For example, “cookies” are small pieces of text which web browsers store on a user’s computer. The cookie registers with the web browser each time the user accesses it and can be used for monitoring activity, for example through session tracking, storing site preferences, authentication. Users can decide whether or not to accept cookies, but some sites become unusable without them. On the whole, tools like these are used to help services providers tailor services to meet people’s needs, for example with online retail sites recommending items that users might be interested in based on analysis of items that they have previously purchased or looked at. However, these tools can also be used to monitor internet users for less benign purposes.

Watching and locating people offline has also become much easier using ICTs. CCTV cameras and satellites are used to monitor public and private spaces, and are available to more and more people through falling prices and private sector initiatives such as GoogleEarth. Other ICTs can be used to track individuals. For example, Global Positioning Systems (GPS) are incorporated into more and more consumer devices. Radio-Frequency Identification (RFID) tags are another example. These are currently prohibitively expensive, but if prices were to fall they could identify, for example, the product that a consumer buys, how often it is used and where (Privacy International, 2006). Again, such technologies have positive uses, but can also encroach upon privacy rights.

Authoritarian governments have been able to use these technologies to monitor the actions of their citizens, particularly dissidents, much more intensively. For example, the OpenNet Initiative reports that in China the most popular online instant messenger (QQ) records users’ online communications and reports on these to the police. In 2008, a Chinese state-owned mobile phone company revealed that it had unlimited access to its customers’ data and that it supplies this to the Chinese government on request (ONI, 2009).

This is not only a problem in countries with limited human rights protections. The UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism has noted examples of excessive citizen surveillance and monitoring in Germany, Colombia, Bangladesh and the USA (Human Rights Council, 2009). A 2007 Privacy International study revealed an overall worsening of privacy protections and safeguards, together with an increase in the occurrence of surveillance across 47 countries.

Surveillance technologies can also be used much more locally, to monitor behaviour of family members and of employees. Instead of only monitoring employees who exhibit suspicious behaviour, analysts suggest that an increasing number of employers are instituting continuous systematic surveillance in the workplace (Schulman, 2001).

3.2.2 Assisting in the consolidation and analysis of personal information

The power of computers and data processing technologies has rapidly increased in recent years, meaning that vast quantities of information, once collected, can be cheaply and efficiently stored, consolidated and analysed. The potential for privacy violations increases exponentially as technologies
are combined together, for example, linking facial recognition databases with closed circuit television (CCTV) cameras would allow tracking of individuals on an unprecedented scale.

The practice of merging and consolidating different informational databases is pervasive, with growing international markets for the sale and purchase of personal data profiles. Combined databases have numerous uses. They can be used for data mining, which is “the process of finding patterns in information contained in large databases” (Fayyad, 2000). Data mining itself has many positive uses, including identifying patterns which indicate fraudulent credit card use. However it can also have significant privacy implications. The practice often involves using people’s information in a way that they did not consent to and are not even aware of. Furthermore, the wide array of data drawn upon often includes personal details and can easily be linked to individuals. Combined databases can also be used for data profiling - the use of aggregated data to build comprehensive profiles on individuals.

In order to protect privacy and comply with privacy laws, companies often de-identify or anonymise the data that they collect through stripping it of personal identifiers such as name, social security number, and IP number. However, studies reveal that it is often possible to relate ‘anonymised’ information back to an individual. For example, in 2006 AOL released data concerning the terms used by its search engine customers. This data was supposed to be anonymised, but researchers were able to identify many users through “vanity searches”, in which individuals search for their own name to see where they are referred to on the web (Soghoian, 2007).

Data profiling is also used in international efforts to fight crime and terrorism. Watchlists of suspects are a key tool in the global battle against terror. However, misinformed data profiling can lead to innocent people being treated as suspects without necessarily having been convicted of anything or given the opportunity to defend themselves. Hosein (2006) argues that many powers created for use in extreme and emergency situations often end up being used for lesser purposes, for example with powers created to tackle terrorism in the UK subsequently being used for minor crimes such as the illegal dumping of waste. Whilst states have an obligation to protect the security of their citizens, there is a danger that the mechanisms being employed are disproportionate, and often without a solid basis in law.

### 3.2.3 The difficulties of protecting personal data in the digital age

Databases can be very hard to protect, especially when they can be accessed remotely and when many people are granted access. The characteristics and nature of digital data exacerbate risks to the right to privacy. For example, it is much harder to destroy digital data than physical data because information is often recoverable, and can easily be reproduced and stored simultaneously in many different locations. Communication networks are also generally difficult to secure, making them vulnerable to hackers. This problem is even more significant on the internet as it is a global network. It is easy for users to send information across the network to countries with lower privacy standards, and if standards are broken in another country, it is harder to prosecute the offender.

Information can also be stored in, or released into, the public domain. This is often for legitimate reasons, but can raise privacy concerns. For example, the international WHOIS database contains the personal contact details of the individual or organisation that have registered any domain name on the internet. The information is publicly available to allow network administrators to easily remedy problems on the internet (EPIC[d]). However, this also reduces opportunities for anonymous speech online, allowing people to track down and put pressure on individuals who are publishing content that is deemed to be undesirable. In many cases, such content may be legal and in the public interest, yet simply offend certain individuals or companies.
As increasing aspects of everyday life depend on digital communications and data processes, it is harder for individuals to control access to their personal data and to know who is accessing and using it. Many people are unaware about how much information is collected about them online. Even if they are aware, information which seems innocuous can actually reveal a great deal. For these reasons, privacy advocates have often criticised the privacy policies of popular websites. Many have been accused of being unintelligible and hidden, making it more difficult for users to make informed decisions about what data and permissions to provide. Technological tools do exist which can help users to protect their privacy such as anonymizers and proxy servers. However, these tools are not always effective, and nevertheless require a level of technical knowledge above that of the average user.

### 3.3 The use of personal data for commercial purposes

#### 3.3.1 Privacy concerns over the activities of internet intermediaries

Internet intermediaries are the range of actors, services and applications that facilitate transactions between third parties on the internet, including for example search engines and ISPs. Internet-based communications are increasingly reliant on these intermediaries for accessing, processing and transmitting data. The increasing power of intermediaries, and their control over personal data, has given rise to a number of concerns about whether current regulation is sufficient to protect privacy rights. This section gives a brief overview of the issues relating to a selected number of key intermediaries.

##### 3.3.1.1 Social Networking Sites

Social networking sites are websites that focus on building and/or reflecting social relations among people. Some facilitate virtual “friendships” with people who are already known to the user offline, allowing them to share photos and chat online. Others concentrate on allowing people to make new friends, often with a particular focus such as work relations (LinkedIn) or music tastes (MySpace). Each service is different, but the standard format allows users to create their own webpage containing various pieces of personal information (such as date of birth, location, interests, name). Users can then link to friends who will be able to see their information and vice versa. Social networking sites are incredibly popular, with hundreds of millions of users between them. However there has been growing concern over privacy violations caused by such sites. Some concerns relate to media and communications literacy, with many users unaware of the risks involved in revealing personal information to others. Many users do not exercise restraint about who they allow to see their data, and many users are believed to befriend people that they do not know well. This can have considerable implications given, for example, that on Facebook the average user has 130 friends on the site (Facebook, 2010).

The vast majority of concerns relate to the privacy policies and practices of the sites themselves. Privacy policies are usually inconspicuous on a social networking site, discouraging users from finding it or reading it. They tend to be long and written in complicated language which isn’t always comprehensible to the average user. Furthermore, default privacy settings tend to expose a large amount of personal information, requiring additional effort from the user to protect their information (EPICa). Almost all social networking privacy policies state that the policy is fluid and may be altered from time to time, although changes will be posted on the website. In many instances, policy changes have made significant changes to users’ privacy without obtaining prior consent. Policies also tend to be unclear concerning what user information is shared with third parties. Facebook, Myspace and Friendster all affirm users’ rights to decide whether to share their information with marketers on the site, and state that they will not share users’ information without their permission. However, they do not elaborate on what information they provide to third parties in aggregate form and whether that
information can subsequently be disaggregated (EPICa). This issue came to the fore in 2007 when Facebook launched a platform that allows users, including companies, to design applications and tools that can be installed and used by Facebook members. Options to withhold personal data given to users of these applications were pre-selected by default, and Facebook has legally exempted itself from liability for how applications providers use this data (EPIC).

3.3.1.2 Cloud Computing

Cloud computing is an emerging network architecture whereby data, processing power or software is stored on remote servers, as opposed to an individual’s computer, and made accessible via the internet (the cloud). Different forms of cloud computing exist, providing a range of services. Individuals or organisations can effectively rent computing capacity from remote service providers. For example, Google’s Apps service allows people to create and save spreadsheet and word processing documents online. Other services include collaborative platforms that allow users access to documents simultaneously, such as wiki platforms, and web-based email services such as Hotmail or Yahoo! (EPICb).

Cloud computing can yield a number of positive benefits. For example, it can reduce the costs of buying and updating software for small businesses and organisations, which can be particularly empowering for users with low levels of financial resources in developing countries. It can also improve convenience for users through allowing them to access documents anywhere in the world, and collaboratively author documents with people working in other geographical locations.

However, cloud computing also raises a number of concerns from a privacy perspective. As data is stored on a third party’s software, the responsibility for protecting that information lies with the third party, and users lose a degree of control. Additionally, laws covering cloud computing are not well defined so users are not assured of the confidentiality or privacy of their data. The terms and conditions (T&Cs) of use sometimes state that the service provider is able to terminate accounts or remove/edit content at their own discretion. For example, this is the case for Mozy.com, a service that allows users to back up the information stored on their PCs online (EPICb). This presents the danger that users could lose their personal information. Many T&Cs strictly limit the liability of the service provider, which could mean that should there be a breach in security and users lose their personal data, they may not have access to any compensation. Finally service providers often do not address what happens with a user’s information once they have deleted the account. This does not always mean that information is removed, potentially leading to privacy breaches (ibid).

3.3.1.3 Search Engines

Search engines fulfil a crucial role as intermediaries on the internet, allowing individuals to find and access content. Examples include Google, Bing, Ask.com, and Yahoo! Search. Search engines typically collect a large amount of personal data including IP addresses, search requests, together with the time, date and location of the computer submitting the request. As discussed above, this information can be personally identifiable and can reveal particularly sensitive pieces of information such as a person’s political beliefs, sexual orientation, religious beliefs and medical issues. This information is generally used for marketing purposes, and there are also risks of public disclosure of information, such as AOL’s release of information in 2006 discussed above. The risks for privacy and other human rights are all the more significant in countries with limited protections for human rights.

As with social networking sites, privacy policies are usually inconspicuous, not easily intelligible, and subject to change. There are also low levels of user awareness about the risks to privacy. A 2006 study found that of 1000 Google users, 77% believe that it would not be possible to gain insight into their personal identities through analysis of the search terms that they have used (EPICc).
3.3.2 Privacy and data protection regulation

There is considerable commonality between national and international privacy and data protection standards across the globe as a result of the emergence of a de facto framework of “Fair Information Practices”. This is rooted in the landmark 1974 Privacy Act in the USA which put limitations on the collection, use and dissemination of personal data held by government agencies (Rotenberg, 2001). The provisions contained in the act formed the basis of the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. They are also reflected in the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108, 1981), the only legally-binding treaty concerning data protection that is open to ratification by all states around the world.

Despite the emergence of international best practice standards for data protection, there is still progress to be made towards the harmonisation of national laws. Online companies still find it hard to navigate the complex patchwork of national privacy laws when operating international internet services than span national boundaries. Privacy advocates are concerned that international standards are being lowered to the lowest common denominator, particularly since the internet environment is dominated by US-based companies who are subject to lower data protection standards than their European counterparts. As the only international legally binding treaty, they call for all countries to ratify the Council of Europe Convention 108 (Madrid Privacy Declaration, 2009). This is particularly important, given the trend towards increased data collection and sharing in the wake of the “war on terror”, which are discussed below.

The EU Data Protection Directive (1995) follows the Council of Europe Convention 108 in prohibiting the transfer of data to countries that do not have adequate data protection laws. However, there are concerns that the requirement that the protection be “adequate” may not be sufficiently rigorous, particularly in the light of agreements between the United States and the European Union on sharing information about international financial transactions and international air passenger records. The 2000 Safe Harbor Agreement with the United States is also controversial, allowing US companies to voluntarily self-certify to adhere to a set of privacy principles agreed between the European Commission and the US Department of Commerce. Once self-certified the companies are presumed to provide “adequate” protection, and can receive personal information from the EU. The agreement has been criticised for assuming the companies provide rigorous protection, for the open-ended grace period for the companies to implement the principles, for the lack of enforcement or systematic review of compliance, and for the lack of individual right to appeal or compensation for privacy infringements.

These agreements have been particularly contentious as the United States approach to data protection legislation is widely regarded as inadequate. The US uses a sectoral approach whereby there are no overarching governmental regulations, but rather legislation is adopted on an ad hoc basis. One major criticism is that laws are specific and so do not cover new technologies, therefore whenever a new technology is introduced there is a period of data insecurity. The sectoral approach is based on the idea that the private sector should lead in this area and that companies should implement self-regulation. However, industry led codes have tended to “provide only weak protections and lack enforcement” (Privacy International, 2006).

---

10 The Madrid Privacy Declaration was signed by 111 privacy organisations and 188 individuals from across the world, designed to coincide with the 31st International Data Commissioners Conference in 2009.
Through enshrining the EU Charter of Fundamental Rights into law, the Treaty on the Functioning of the European Union (Lisbon Treaty) of 2009 established data protection as a fundamental right of European citizens. The Treaty also contains a specific provision (Article 16(2)) to “develop a comprehensive and coherent framework for the protection of personal data” (Reding, 2010). The process of reforming the 1995 Data Protection Directive is currently underway, with Commissioner Reding stating that “reinforcing the confidence of both citizens and businesses in data systems will lead to better protection for individuals, as well as to trust and confidence in new services and products” (ibid). The new framework is expected to address “new challenges of the information age, such as globalisation, development of information technologies, the internet, online social networking, e-commerce, cloud computing, video surveillance, behavioural advertising, data security breaches, etc” (ibid). A review of European data protection measures conducted by the Article 29 Data Protection Working Party (2009) found that the original principles of the Directive are still valid. However, it argued that they would benefit from better application and harmonisation of rules, and that the addition of new innovative principles should be considered. These include “privacy by design principles” which would incorporate technological data protection safeguards into ICTs at the planning and design stages.

3.4 Surveillance and data protection to increase public security

Following the increased international efforts to enhance security and eradicate terrorism in the wake of the events of 11 September 2001, human rights advocates have reported “a dramatic increase of the storage and exchange of personal data in relation to activities of the police and justice sector” (Article 29 Data Protection Working Party, 2009:26). Trends have included: increased use of surveillance, increased data sharing between governments and third parties, and the retention of data for extended periods of time (Human Rights Council, 2009).

International human rights law does permit certain civil and political rights to be restricted to protect national and individual security. However, restrictions must be strictly proportionate, prescribed by law and necessary in a democratic society. The Siracusa principles of 1984\(^\text{11}\) state that “national security cannot be invoked as a reason for imposing limitations to prevent merely local or relatively isolated threats to law and order” and “cannot be used as a pretext for imposing vague or arbitrary limitations”. The question therefore arises as to whether current regulation and approaches to addressing cyber-security issues are in line with these principles.

Political discourse at international and national levels tends to stress the potentially harmful aspects of digital communications over their empowering characteristics. The internet is a readymade global communications network which is relatively cheap and simple to use. It was also initially designed to be resilient to attack, with inbuilt redundancy. If one section of the network is damaged or destroyed, the communication system as a whole can still function as data is simply routed through different sections of the network. It is similarly difficult to shut down online communication networks used by subversive groups which are themselves organised in resilient network structures. The anonymity and obscurity of online communication can be enhanced by the use of encryption and steganography, and traceability can be limited by the use of public internet access points, proxy servers\(^\text{12}\) and onion routing\(^\text{13}\).

---

\(^{11}\)Siracusa Principles on the Limitation and Derogation of Provisions in the International Covenant on Civil and Political Rights. [http://graduateinstitute.ch/faculty/clapham/hrdoc/docs/siracusa.html](http://graduateinstitute.ch/faculty/clapham/hrdoc/docs/siracusa.html)

\(^{12}\) Proxy servers act as intermediaries between the location from which the user is accessing the internet, and the server that they are accessing information from. They can help to enhance the
However, characteristics that make the internet attractive to criminals are also the very characteristics that make it a powerful tool for human rights defenders in repressive regimes. It is therefore all the more important to be careful in assessing whether it is necessary to control communication flows and online activity in order to protect national security. In order to do this, it is first necessary to assess the nature and extent of potential and actual threats. These can be divided into three broad categories: cyber-extremism and terrorism, cybercrime and state-sponsored cyber-attacks.

### 3.4.1 Cyber-extremism and terrorism

Much attention has been paid to the role that the internet and other ICTs play in fostering political extremism and facilitating terrorism, both within national and international policy discussions and within popular media and discourse. As Kofi Annan commented, “the same Internet that has facilitated the spread of human rights and good governance norms has also been a conduit for propagating intolerance and has diffused information necessary for building weapons of terror” (Annan, 1999). Cornish (2009) describes how ICTs can be used to assist subversive activity in a number of ways. Firstly, ICTs are powerful tools for mobilisation and recruitment. Websites, blogs, chat forums, social networking and SMS messaging can be used to spread information about extremist causes and recruit people to join subversive networks. Secondly, ICTs can be used to organise members of these networks, providing tools and platforms for planning subversive activities. Thirdly, the internet hosts a wealth of information that can be of use for training and planning terrorism. For example, training manuals can be uploaded and shared and the increasingly detailed and sophisticated maps that are available online can be useful tools for planning terrorist activities. The internet also provides spaces and tools for training activities, for example with online simulators and role playing games being used as “virtual training camps” for terrorism (ibid). Finally, the internet itself is a virtual battleground of ideas and norm creation, with battles to win over hearts and minds being fought around the clock on blogs and virtual forums across the Web.

ICTs thus offer a range of tools, platforms and resources for mobilising and organising, and the characteristics of internet-based communication networks enhance the usefulness and power of these for extremist and terrorist activity. However, it is important to distinguish between the potential use of ICTs for criminal activity, and the actual use. There is a lack of empirical evidence concerning the effectiveness of online mobilisation and the impact that the evolution of ICTs has had on the number, scale and effectiveness of terrorist attacks (Conway, 2005). A number of analysts argue that the threats that cyber-extremism and cyber-terrorism present to national security have been exaggerated in formal and popular discourse. Kimmage (2008, quoted in Cornish, 2009) argues that terrorist networks use ICTs because they have to rather than because they choose to; it is a sign of weakness rather than strength. Similarly, McAllister (2004) claims that centralised bureaucracies are more efficient at planning and executing activities than networked structures. The dispersion of nodes in networks makes coordinated planning difficult, flows of information inefficient and duplicative, and interception more likely. Face to face mobilisation and planning remain more powerful than virtual methods (Zanini and Edwards, 2001). The argument follows that the power that terrorist groups gain through online networking should not be overestimated.

Anonymity of users, as attempts to trace communication flows will lead the investigator to the proxy server rather than to the IP address of the user.

13 Onion routing is a technique whereby several layers of encryption are added to data being sent across a network. The data is then sent through several nodes in the network which each remove a layer of encryption. The system helps to prevent interceptors from knowing the source, destination and content of the data.
3.4.2 Cybercrime

ICTs support and facilitate a range of criminal activity, from low level hacking to international serious and organised crime. Evidence suggests that the extent and seriousness of online crime is increasing rapidly as the professionalism of the online fraud industry and the sophistication of its tools increase (Symantec, 2009). The most common purpose of organised cybercrime is financial gain, for example with malicious code and programmes being used to expose confidential information that can be used to gain access to bank accounts and other assets. Symantec (2009) reported a dramatic increase of 165% in the number of new malicious code signatures created between 2007 and 2008, from 600,000 to over 1.6 million. They also reported an increase in coordination and trading between organised crime groups, and increasing rates of malicious activity in new countries experiencing escalating volumes of internet traffic that local service providers are unable to monitor effectively.

3.4.3 State-sponsored Cyber-Attacks

A number of high profile attacks on public infrastructure, media and communication channels and state security systems have recently focused government attention on the dangers presented by war waged via the internet and associated ICTs. States are reportedly devoting significant resources to developing systems for cyber-war and cyber-defence. China is often cited as a primary example (see for example Cornish, 2009). Increasing incidents of “cyber-intrusions” and cyber-attacks have been traced back to China although it is not clear whether they have been officially condoned or implemented by the state. Owing to the subversive and sensitive nature of state-sponsored cyber-attacks, it is difficult to gauge their seriousness and the nature of government responses. However, the issue has increased in prominence over recent years, and is likely to enhance ongoing efforts to control and monitor internet-based communications and activity.

A recent research project unveiled an extensive cyber-espionage network operating out of China that compromised the computer systems of governments, business and organisations across the world, including UN offices and the office of the Dalai Lama (Information Warfare Monitor and Shadowserver Foundation, 2010). The report’s authors call for a global convention on cyberspace that “builds robust mechanisms of information sharing across borders” and that requires states not to tolerate “mischievous networks” operating out of their jurisdiction (ibid:ii). They argue that the absence of positive shared norms, principles and rules in cyberspace threatens to undermine the valuable global commons that is the internet through creating a climate of fear on the web and presenting the danger of heavy-handed responses to cyber-espionage.

3.4.4 Promoting a safe and open internet: the need for balance and proportionality

In addition to policy responses to the commercial use of personal data as discussed in the previous section, there have also been a number of recent developments concerning transborder flows of personal information in the name of fighting terrorism. The EU Commission is currently seeking to protect the rights of EU citizens in new negotiations over the sharing of airline passenger records, including pushing for the right to bring complaints in US courts if they believe data has been misused (New York Times, 2010). The Lisbon Treaty established new co-legislation powers for the European Parliament on data protection in police and judicial cooperation on international matters, previously the sole domain of the Council. In February 2010 the Parliament exercised these new powers through voting to reject a 2009 agreement between the Council and the US government to share information about international financial transactions contained in the SWIFT database.

At the global level, perhaps the most significant initiative that has been taken in terms of setting standards and coordinating international approaches to cybercrime is the Council of Europe
Convention on Cybercrime which entered into force in July 2004. Unlike other international guidelines, the Convention is legally binding on its signatories. Moreover, the Convention is open to signature by states that are not members of the Council of Europe, increasing its power and significance (Cornish, 2009). The Convention currently has 29 ratifications or accessions and has been signed by a further 17 states. Most are European, but the Convention has also been ratified by the USA and signed by Canada, Japan, and South Africa.

The Convention has three main parts. The first proposes that online activities and data interference, copyright circumvention and computer fraud are criminalised. The second requires states to enhance domestic surveillance for the investigation of criminal activity. The third requires cooperation between states for criminal investigations (Privacy International, 2004). The text of an Additional Protocol to criminalise “acts of a racist and xenophobic nature committed through computer systems” was finalised in 2002, and entered into force in 2006.

The Convention has been heavily criticised by a number of organisations and groups concerned with the protection of civil liberties (Privacy International, 2004). From a human rights perspective, the main criticism of the Convention is that it does not contain adequate safeguards for the protection of privacy or limitations on the use of privacy invasive technologies. This has led human rights advocates to express serious concerns that “the Convention does not seem to be compatible with the European Convention on Human Rights and with the jurisprudence of the European Court of Human Rights in Strasbourg especially in relation to article 8” (Akdeniz, 2008:10).

A significant concern is that the Convention allows party states to request data gathered by other parties without any dual criminality requirements. This is particularly problematic as the Convention is open to ratification by states outside of Europe with less rigorous data protection laws. States are obliged to cooperate in the investigation of activities that are illegal in other countries, but legal in their own. This presents the danger that the treaty will be manipulated for political reasons, which may have serious implications for legitimate political association and protest (ACLU, 2003). The treaty has also been accused of being too broad, placing more restrictions on online activity than are present in the offline world, and giving states more pervasive controls over online communication than offline (EDRi, 2007).

In short, the Cybercrime Convention does not achieve an acceptable balance between promoting security and promoting human rights, in particular privacy. There is not scope within this paper to examine the range of other national and international approaches to cyber-security. However, the Convention is already starting to act as a global set of norms for tackling cybercrime, and human rights analysts agree that, in general, very little attention is given to human rights in the formulation of national cyber-security policy and approaches. A recent Resolution from the Council of Europe itself stated, “in some cases, anti-terrorism legislation restricting freedom of expression and information is too broad, fails to define clear limits to authorities’ interference or lacks sufficient procedural guarantees to prevent abuse” (CoE, 2009: 11).

Privacy advocates are concerned that these developments are eroding international standards, arguing that privacy law and institutions have not paid adequate attention to new surveillance practices, many of which have been facilitated by advancements in ICTs such as biometric identifiers and advanced behavioural targeting (Madrid Privacy Declaration, 2009). They call for an independent and transparent

---

14 There is not scope within this paper to discuss the full range of approaches being taken by different bodies at international and national levels. For a review of OECD, ITU and EU policy in this area, see Cornish (2009).
evaluation of new systems of mass surveillance, and the establishment of a new international framework for privacy protection, based on the rule of law, human rights and support for democratic institutions (ibid).

### 3.5 Conclusions

Privacy is an important right within the human rights framework, not least because it helps to support expression and other fundamental freedoms through protecting the anonymity of communicators. This is particularly important for people in repressive regimes with few protections for human rights. However, privacy is a qualified right, and a careful balance has to be struck between protecting public security and protecting privacy rights. At international and national levels, there has been a trend towards the increasing erosion of privacy rights in the name of enhancing security and fighting terrorism. From a human rights perspective, approaches taken are often disproportionate. Europe has an important role to play in promoting a proper balance between civil and political rights and security at international and national levels.

It is natural that states are taking measures to limit the use of ICTs for illegal activity, and in some instances human rights law actually requires states to be proactive. However, it should be remembered that the same characteristics and tools that make the internet attractive for criminals have helped to enhance freedom of expression and associated rights and goods through facilitating the evolution of open, participative and collaborative communications environments. Tools to enhance anonymity are not only useful for criminals, but also for human rights activists and everyday internet users seeking to circumvent political and social censorship.

Human rights analysts suggest that many of the responses to tackling criminal behaviour online have been driven by moral panic and have been disproportionate to the threat at hand (Akdeniz, 2008; Powell et al., 2010). This is not only damaging to the human rights of citizens of democratic countries, but also for people who are fighting for democracy and human rights in countries across the world. In the current global climate of the war on terror, democratic countries cannot afford to be exporting bad practice. This not only provides a smokescreen for the explicit violation of human rights in authoritarian countries, but also sets global norms that are detrimental to the global human rights movement. As a resolution adopted by the Council of Europe Ministers responsible for Media and New Communications Services states:

> “Freedom of expression and information risk falling victim to terrorism, due to a climate of fear that terrorism can create or as a side effect of anti-terrorism legislation or measures. This would be a double success for the terrorists. The freedom of expression and information is, on the one hand, an essential part of the values that terrorism seeks to destroy and, on the other, indispensable to fighting terrorism effectively” (CoE, 2009:11).

In the commercial sector, some of the most revolutionary platforms that have spurred freedom of expression and association have stemmed from an opening up of communication spaces and enhanced information sharing rather than from attempts to protect personal privacy. Collecting data about user activities and preferences has helped online companies to tailor services in ways that are valued by many consumers. However, there is a generally low level of awareness amongst users of communications technology about the ways in which their personal data is being used, and about the implications that it has. Company policies often do little to remedy this situation, disempowering users through damaging data sharing practices, complicated user agreements and default privacy options that favour data protection over privacy protection. Ultimately, it is individuals who should be able to decide where the line should be drawn between the use of their personal data to improve their online experience and their right to limit such use as part of their right to privacy.
The overall aim of policy and regulation in this area should be threefold. Firstly, it needs to empower internet users so that they have both the power to decide how their data is collected and used, and the knowledge and understanding that is needed to make informed decisions. Secondly, it should work to achieve an appropriate balance between privacy, security and openness so that the human rights of all are protected and realised to the fullest extent possible. This will require rigorous research to understand the nature and extent of the threats that digital communications pose to public security, and risk assessment of the damage that responses might cause to human rights and the openness of the internet. Finally, it should seek to clarify the roles and responsibilities that different stakeholders, and in particular the business sector, have across all "layers" of communications environments. This will involve providing positive support for businesses to uphold human rights through their business practice, and working to harmonise regulation to facilitate business on the transboundary medium of the internet. Progress in these areas would help to build communications environments that protect and promote human rights and the public interest for all people.

4 ACCESS TO KNOWLEDGE, CULTURE AND IDEAS: THE DANGERS OF EXCESSIVE COPYRIGHT PROTECTION.

The international human rights framework recognises the benefits that the production and circulation of information, ideas, culture and knowledge have for individuals and society. As discussed in chapter 4, this is reflected in the right to freedom of expression as defined in the UDHR and ICCPR. This chapter focuses on Article 27 of the UDHR and Article 15 of the ICESR which balance the right of all people to enjoy the benefits of culture and scientific progress with the right of authors and innovators to benefit directly from any gains stemming from their work.

This chapter explores the complexities and nuances of this balance, before moving on to examine how it is playing out in the field of digital networked communications. It describes how regulatory and policy focus at the international level has been on providing increasing protection for intellectual property rights rather than on achieving a careful balance between promoting innovation and public access to knowledge. This has served to benefit large companies in the corporate sector rather than consumers and citizens, both in the Western Hemisphere and in developing countries.

To date, the EU has not played a progressive role in balancing between innovation and access to knowledge through its trade, development and copyright policy. The stance the EU has taken in negotiations on the multilateral Anti-Counterfeiting Trade Agreement has been heavily criticised by human rights advocates. However, it is not too late for the EU to play a more positive role in promoting the development of communication architectures, policy and practice that promote innovation, creativity and human advancement. This should be done at national and international levels, in bilateral and multilateral standard setting arenas, and across a range of policy spheres including internet governance, trade and development.

4.1 The right to culture in the international human rights framework

Article 15 of the ICESCR provides the basis for human rights standards relating to access to knowledge, culture and intellectual property. The text of the Article is contained in Box 5.

Box 5: Article 15, UN International Covenant on Economic, Social and Cultural Rights (1966)

1. The States Parties to the present Covenant recognize the right of everyone:
   (a) To take part in cultural life;
   (b) To enjoy the benefits of scientific progress and its applications;
(c) To benefit from the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author.

2. The steps to be taken by the States Parties to the present Covenant to achieve the full realization of this right shall include those necessary for the conservation, the development and the diffusion of science and culture.

3. The States Parties to the present Covenant undertake to respect the freedom indispensable for scientific research and creative activity.

4. The States Parties to the present Covenant recognize the benefits to be derived from the encouragement and development of international contacts and co-operation in the scientific and cultural fields.

Articles 15(1)(a) and 15(1)(b) proclaim public rights to access, take part in the formation of, and benefit from knowledge. This includes not only forms of knowledge that directly help to improve standards of living, such as access to “essential medicines” and “means of food production” (CESCR, 2005:para 35), but also forms of knowledge that make up the various dimensions of culture and human creativity. The Committee on Economic, Social and Cultural Rights (CESCR) has established a broad definition of culture, encompassing inter alia:

“ways of life, language, oral and written literature, music and song, non-verbal communication, religion or belief systems, rites and ceremonies, sport and games, methods of production or technology, natural and man-made environments, food, clothing and shelter and the arts, customs and traditions through which individuals, groups of individuals and communities express their humanity and the meaning they give to their existence, and build their world view representing their encounter with the external forces affecting their lives” (General Comment 17, 2005:para 13).

Through stating that everyone has the right to “take part in” cultural life, the ICESCR envisions people having an active and participatory relationship with knowledge, rather than being mere consumers. In General Comment 21 on the Right to Culture, the CESC states that this encompasses access, participation and contribution, including the rights to “seek”, “develop” and “share” cultural knowledge (2009:para 15). Article 15(1)(c) proclaims, on the other hand, the private right of the authors of knowledge to “moral and material interests” resulting from those creations. This is not just an individual right but also aims to benefit society as a whole by providing an incentive to innovation. As the CESCR states: “[the article] seeks to encourage the active contribution of creators to the arts and sciences and to the progress of society as a whole” (2005:para 4).

The public and private elements of Article 15 can be in conflict. For example, placing emphasis on the creator’s right to benefit from their work could discourage innovation by making the costs of research and development excessively high. Researchers may not be able to afford to access the knowledge on which to build upon. Incentives to innovate may thus be skewed towards goods that will yield significant profits. However, it is not necessarily these goods that the public is in most need of. Examples include malaria medicines in the health sector (Human Rights Council, 2010:para 13), and in-depth analysis of political issues in the media sector.

Placing these, often conflicting, rights alongside each other within the human rights framework “is no accident, but rather an acknowledgment of the inherent tensions between intellectual property protections and widespread access to science and culture” (Shaver and Sganga, 2009:17). It is widely understood that to fulfil Article 15, states must balance these competing interests. However, the exact contours of that balance are not widely discussed or agreed upon (Shaver, 2007).
Historically, there has been much greater emphasis on the private dimensions of Article 15, rather than the public dimensions. This is perhaps because the right to “benefit from the protection of the moral and material interests” of creations belongs to easily identifiable individuals, and industries have developed markets which trade in these rights and whose business models depend on their enforcement (for example, in the media or biotechnology sectors). Powerful lobbies of companies campaigning to protect intellectual property rights have developed at national and international levels, leading policy makers and regulators to focus on protecting copyright rather than on regulating information and culture ownership and control in the public interest. Human rights activists have tended to be less active in promoting economic, social and cultural rights than civil and political rights. Where they have promoted them, they have tended to focus on those rights which are more obviously related to standard of living such as the right to food, health and education. That said, a growing consensus has emerged that human and national development requires, and is enhanced by, broad access to knowledge and culture, and groups have emerged (notably, the Access to Knowledge (A2K) movement) who are increasingly concerned with promoting public rights in this sphere. These groups have tended to embrace all elements of Article 15, promoting not just the economic aspects, but the cultural ones as well.

Because of the strong and generally unopposed intellectual property (IP) lobby, a robust body of international law has developed that protects IP interests. In response to growing concern about the damaging effects that this is having on public access to knowledge and culture, the CESCR issued a General Comment on Article 15 in 2005. The Committee distanced Article 15(1)(c) from IP law, declaring that “moral and material interests... need not necessarily reflect the level and means of protection found in present copyright, patent and other intellectual property regimes” (para 10). The Committee emphasised the importance of the public interest. It stated that, “ultimately, intellectual property is a social product and has a social function” (para 35), and that, “in striking [a] balance, the private interests of authors should not be unduly favoured and the public interest in enjoying broad access to their productions should be given due consideration” (ibid). Finally, the Committee proposed that states should “consider undertaking human rights impact assessments prior to the adoption and after a period of implementation of legislation for the protection of the moral and material interests resulting from one’s scientific, literary or artistic productions” (ibid).

4.2 The right to culture in the age of digital communication

The internet and related ICTs embody and exacerbate the tensions between the public and private dimensions of Article 15 of the ICESCR. On the one hand, the evolution of ICTs has revolutionised the ways in which information is created, accessed, edited and distributed, thereby enhancing opportunities for the realisation of the right to culture and access to knowledge for human and social advancement. Content can be created more economically and easily than ever before. It can be accessed by billions across the globe via the internet, through computers (at home or in community locations) and through newer mobile technologies, such as 3G phones. Platforms have developed whereby everyone can contribute to the development of knowledge, with the most famous example being the collaboratively authored encyclopaedia Wikipedia. Once content is created it can be distributed widely, cheaply and speedily at the click of a button. Significantly, these technologies have allowed the general public to move from users of information and consumers of culture to creators, via blogs, forums, user news, Youtube, digital music mixing platforms and other ICT tools.

On the other hand, digital technologies have made it vastly easier for people to violate copyright. In the past, previously high costs of reproduction and distribution, together with decreasing quality of copies, acted as natural barriers to widespread copyright violations. However, the technologies described above also allow individuals to copy digital material indefinitely, with no loss of quality, and to
distribute copied materials widely, cheaply, and speedily (Schonwetter, 2006). Industries that depend on strong copyright protections to support their business models have understandably sought to protect their market position, and have developed many techniques, technological, legal and otherwise, to prevent violations of their copyright. Digital Rights Management (DRM) is a generic term for controlling access to digital content. The most common forms of DRM are outlined in Box 6.

**Box 6: Common forms of DRM**

*Click–wrap licensing.* A common technique has been for companies to adopt a form of licensing which prevents users from accessing their products without accepting non-negotiable terms. For example, when installing software on a computer, it is usual for a software licence to appear on the screen and to forbid a user from continuing without indicating acceptance of the terms. Given the unequal bargaining power of the parties to such contracts, it is not uncommon for companies to include conditions which are more onerous than those required by law. An example occurred in Norway where a user’s DVD forbade him from making personal copies despite this being allowed under Norwegian law. The user took the case to the court which held that the buyer was subject to the less restricting requirements of the national law and was allowed to make personal copies (Bing, 2005:209).

*Paying for Content.* Some content providers are starting to charge for information online, for example newspapers, which have thus far almost always been freely available in digital formats (see Rupert Murdoch’s August 2009 announcement that he intends to start charging for access to News Corporation’s newspaper websites (BBC News, 2009a)). Charges tend to be fixed and not subject to national contexts, and so prices are often beyond the reach of consumers in developing countries. This technique is not limited to news content; many large educational publishers charge high subscription fees for access to their research and journals, even when some of the content is clearly publicly-funded (Armstrong and Ford, 2006:5). This form of access can be more prohibitive than print access. For example, a library user’s access to a particular online journal can change year on year depending on whether the library can afford the annual subscription, whereas in the past hard copies once bought could be accessed in perpetuity (ibid:6).

*Technological Protection Measures (TPM).* TPMs are technological ways of locking up digital information and can be grouped into two categories: those that limit access to protected content (using, for example, passwords, digital signatures or cryptography), and those which seek to control use of protected content (such as scrambling systems on DVDs that prevent third parties from reproducing them) (WIPO[a]). These measures have been particularly controversial because they fail to distinguish between uses which are fair (such as a school copying a DVD so it can be shown in different classes) and piracy.

Through affecting both the private and public dimensions of Article 15 of the ICESCR, ICTs by themselves do not in themselves upset the balance between the rights of authors and the rights of consumers of, and “participants” in, cultural and scientific knowledge production. However, there is a discernible trend at national and international levels to enhance legal intellectual property rights to such an extent as to threaten both innovation and the opportunities that ICTs present for advancing rights to culture, knowledge and expression. This is largely due to the power of multinational companies in the medicine, media and cultural industries whose business models depend on copyright protection and are threatened by enhanced knowledge and cultural exchange facilitated by ICTs. The distribution of IP rights is skewed at the global level, with the overwhelming majority being held in a few leading countries with high levels of technological development (Human Rights Council, 2010. See also Figure 3 which shows that the wealth deriving from intellectual property rights is located overwhelmingly in the global north). In these countries, the IP industry often contributes a significant
amount to the national economy. This has lent them significant lobbying power at national and international levels, with governments actively pushing for ever stronger IP protection laws and practices on the international stage.

The economic and political power of many IP holders in the corporate sphere vastly outweighs that of individual ICT users and small service providers, placing the latter groups at a major disadvantage when accused of violating copyright through their cultural and expressive activities online. There is evidence that some IP holders make misleading copyright claims, for example through sending notices or letters to users and website owners threatening criminal penalties without acknowledgement of fair use or relevant exceptions and limitations (Information Society Project, 2008). The receiver will often automatically take down relevant information, or refrain from certain actions, to avoid costly legal action or because they are not aware of their rights. Within ICANN\(^\text{15}\), consumer groups are concerned about the disproportionate power that corporate lobbies have over the management of critical internet resources such as the distribution and governance of domain names (see for example Mueller, 2009).

Whilst companies are entitled to a degree of copyright protection of their scientific and cultural produce, the international IP regime currently works to protect the interests of big business rather than the rights of individual authors. This reduces overall levels of innovation and creativity from which society can benefit, and restricts access to knowledge and culture that is in the human and public interest.

4.3 Upsetting the balance: International trends in intellectual property rights protection

4.3.1 Enhancing online copyright protection at the national level

IP-rich countries have been enacting ever stronger laws at the national level to combat copyright infringement. One significant trend is the increasing use of criminal penalties for ordinary copyright infringements. On the internet, this has including proposals for “three strikes” rules\(^\text{16}\) or “graduated responses” whereby repeat copyright violators are disconnected from the internet if they ignore warnings, usually without judicial process and oversight. For example, in May 2009, France adopted the Loi favorisant la diffusion et la protection de la création sur Internet or HADOPI law. A central and controversial initiative of the bill was that internet users accused of copyright violations could be disconnected from the internet on a third warning. The user did not have to be convicted in court of copyright violations for this punishment to result. This initiative was struck down by the French Constitutional Court in June 2009 which stated that users can only be disconnected from the internet if the case is reviewed judicially, in order to respect the presumption of innocence. The bill was amended to include the judicial review requirements on 22 October 2009. A similar law exists in South Korea (Article 133 of the Korean Copyright Act July 2009) and in the UK (The UK Digital Economy Act, passed April 2010). One is also being debated in Belgium (a “four strikes” rule).

\(^{15}\) The Internet Corporation for Assigned Names and Numbers, the private institution responsible for assigning Internet Protocol addresses and domain names at the international level.

\(^{16}\) “3 strikes” is an analogy drawn from baseball. It is commonly used in online copyright protection to refer to cases in which customers suspected of copyright violation are given three warnings to refrain by their ISP. If they ignore these warnings, internet access is suspended.
"Three strikes" rules have been widely criticised. Many groups view the internet as far more than a luxury, but more akin to a vital service given its necessity for many fundamental public goods and activities such as work, education, leisure, and political involvement (see chapter 8 on equality and the principle of non-discrimination for further discussion). Accordingly, some believe disconnection is never a suitable penalty, whilst others believe that it can be used but only in extreme circumstances and following a conviction in court. Disconnection is also criticized as an indiscriminate punishment which, when pursued, affects everyone using that IP address. This could be a whole family or household, or whole communities in the case of communal internet access points such as libraries or internet cafes.
The EU parliament has also shown concern about this issue. The European Telecoms Package entered into force on 19 December 2009 and member states are required to implement the Directive into national legislation by June 2011. The Directive was much debated. The European Parliament was particularly concerned with the use of internet disconnection as a penalty for users. An amendment was inserted by the Parliament (Amendment 138 and later 46) which provided that internet access could only be restricted following a prior ruling by the judicial authorities. This amendment was inserted on the understanding that access to Internet is a fundamental right (as declared by European Commissioner Viviane Reding). The Council of Ministers twice rejected this amendment, initiating the conciliation process. Finally, the Parliament and Council agreed for softer requirements within a so-called "internet freedom provision", namely that internet restrictions can “only be imposed if they are appropriate, proportionate and necessary within a democratic society” and with the possibility of judicial review (European Parliament, 2009).

Another related trend has been the augmentation of the legal responsibilities of ISPs in addressing copyright violations. In many countries (such as in the US and EU countries) ISPs are granted legal immunity for prosecution for illegal activities carried out by users of those services, provided that on receiving notice from a copyright holder that their network is hosting infringing material, they expeditiously remove or disable access to that material. This system is known as “notice and takedown”. If the ISP believes the material does not infringe on any copyright, they are entitled to refrain from removing the material. In this way the system is supposed to self-police and ensure that only infringing material is removed. However, it is likely that in most cases on receiving notice, ISPs will simply take down the material to avoid any likelihood of incurring expensive legal actions. This situation allows wealthy copyright owners to make misleading copyright claims to remove any displeasing material. For example, in 2003 a German comedian was ordered to take down his parody website about the German Federal Chancellor. The notice he received accused him of infringing on the Chancellor trademark, even though it was used in a clearly comic way, which would widely be considered fair use (EDRI, 2003). On this occasion the notice recipient questioned the validity of the notice claim, but this does not always happen.

4.3.2 Expanding the scope of copyright protection at international levels

There are many international treaties establishing copyright law, but the three which are widely regarded as the most relevant in this field are the 1886 Berne Convention (revised at least six times, most recently in Paris in 1971), the World Trade Organisation’s TRIPS Agreement of 1995 and the World Intellectual Property Organisation (WIPO)’s Copyright Treaty of 1996 (see Consumer International, 2006). In effect, each of these treaties have expanded the scope of copyright protection in terms of the materials which are protected, the rights of authors, and the duration of those rights. For example, the Berne Convention defined the works which could be protected by copyright as “every production in the literary, scientific and artistic domain, whatever may be the mode or form of its expression” (Art 2(1)), including translations, adaptations and compilations of material. This definition was copied and extended by the TRIPS Agreement which added “computer programs” (art 10(1)) and “compilations of data or other materials (Art 10(2)) to the protected list, effectively updating it for the information age.

Whilst the Berne Convention initially granted protection of IP rights for the duration of the author’s life and seven years after his/her death, this has now been amended to the author’s life plus an additional 50 years, with advice being issued by WIPO that 70 years is now becoming the global norm (Consumer International, 2006:21). This is in stark contrast to the first conception of copyright protection in the UK

17 TRIPS stands for trade-related aspects of intellectual property rights.
in 1709 which gave 14 years of protection to new publications and a further 14 years if the author was still alive after this period (The Economist, 2010). The timescales of protection were intentionally short in order to “nurture and channel the spate of inventiveness that Enlightenment society and its successors have since enjoyed” (ibid:16).

Whilst international trends point towards more stringent copyright protection, the international IP regime does include a number of flexibilities in the form of exceptions and limitations which countries can use to adapt their national legal frameworks to benefit national and community culture. Exceptions are commonly called ‘fair use’ and include uses such as classroom use, format conversion, making personal copies, library lending, reviews and critiques, research purposes and sampling (see Information Society Project, 2008:6). Flexibilities have been inserted into many legal systems, for example through the fair use concept in the US legal system or the list of optional exceptions in Article 5 of the EU Copyright Directive. However, despite the potential of such exceptions to promote cultural participation and innovation, they are not widely used in developing countries, largely due to pressure exerted by IP-rich countries during trade agreement negotiations.

4.3.3 Restoring the balance? The WIPO Development Agenda

WIPO is the specialised agency within the UN that was established in 1967 to “promote the protection of intellectual property through the world” (Convention establishing WIPO, Art 3(i)). WIPO is mandated to provide technical assistance to countries in developing their IP rights systems. As human rights do not feature in the WIPO mandate and very little coordination exists between the organisation and the UN’s human rights bodies, assistance is not directed to designing suitable IP regimes that protect human rights through the establishment of limitations and flexibilities, but rather solely to developing robust regimes that enforce IP rights (Gold and Morin, 2009).

Following a campaign spearheaded by Brazil and Argentina, in 2007 the WIPO General Assembly adopted a set of 45 recommendations known as the WIPO “Development Agenda”. The recommendations cover public interest themes such as technical assistance and capacity building and ICTs and access to knowledge. They aim to make WIPOs work and legal framework more development-orientated through, for example, recognising that each country has a unique situation and supporting the use of flexibilities (Recommendation 14) and providing technical assistance accordingly (Recommendation 1).

WIPO’s Development Agenda is somewhat new and an analysis of its achievements by the Human Rights Council determined that progress so far has been “somewhat slow” (2010:7). Analysts suggest that this is at least in part a result of a prevailing mindset within WIPO that its obligation is to further IP protection above other social goals, as well as other factors such as a lack of human resources (Gold and Morin, 2009). Despite this, the establishment of the Development Agenda has been heralded as a momentous achievement for WIPO with regard to improving the balance between private and public rights in this sphere. The Human Rights Council proclaimed it to be “one of the most – and arguably the most - important of the current global initiatives in advancing the realisation of the right to development” (2010:4).

4.3.4 Undermining progress: "TRIPS plus" and ACTA

In bilateral and multi-lateral trade negotiations it is very common for IP-rich counties to require other countries to commit to adopting IP enforcement mechanisms which are above the requirements of TRIPS, therefore known as "TRIPS plus" (Armstrong and Ford, 2006). At the time of writing, the most important and controversial multi-lateral agreement concerning IP rights is the Anti-Counterfeiting Trade Agreement (ACTA). This is a proposed trade agreement between the US, Japan, the European Commission, Switzerland, Australia, Canada, Jordan, Mexico, Morocco, New Zealand, South Korea and
the United Arab Emirates. The final terms of ACTA are due to be agreed this year, following seven rounds of negotiation which commenced in October 2007.

ACTA is widely criticised by a number of stakeholders because it is being negotiated in secret, excluding civil society, accountability institutions and most developing countries and there are no mechanisms made available for feedback on proposals.

Speculation about what might or might not be included in the agreement was based on numerous leaks. The European Parliament had unsuccessfully requested a copy of the draft agreement from the European Commission on numerous occasions. In March 2010 the Parliament issued a resolution “deplor[ing] the calculated choice of the parties not to negotiate through well-established international bodies, such as WIPO and WTO, which have established frameworks for public information and consultation” (2010b:para 6). It “call[ed] on the Commission and the Council to grant public and parliamentary access to ACTA negotiation texts and summaries” (ibid:para 3). As a result, in April 2010, ACTA negotiators finally released the draft text having removed attribution to country positions. This highlights the value of public pressure, and provides an example of an effective tool that the European Parliament can use.

Fears that ACTA would make graduated response penalties mandatory have been alleviated as a footnote contained in leaked documents which proposed graduated response as a model policy, have been removed. There are still concerns that ACTA may be used to encourage third countries to adopt this policy as proposed text specifically states that such a policy is not in conflict with the agreement (Geist, 2010).

Other fears have been confirmed, namely that ACTA seeks to develop a regulatory IP regime more onerous than that which currently exists at the international level, including controversial “TRIPS plus” provisions. The draft ACTA calls for the increased use of criminal and civil penalties against people using copyright circumvention technologies and those accused of copyright infringements, and also for ISPs to have more responsibilities with regards to removing infringing material.

As already discussed, these provisions are dangerous, potentially offering limited protections for access to knowledge, information and culture in the public interest. There are also concerns that ACTA is not merely seeking to bind the negotiating states, but is also creating a new international standard which is likely to be imposed on third countries in future trade agreements, possibly even replacing WIPO (Geist, 2010a). The draft text indicated that there is still disagreement over many of the terms of the agreement.

Encouraging innovation and protecting rights to knowledge and culture: Alternatives to enhancing intellectual property rights

In the face of increasingly restricted legal access to knowledge and culture, civil society actors and innovative businesses have been developing dynamic alternatives to formal copyright. Some of the most significant initiatives are described in Box 7. The underlying rationale of these approaches is that overzealous protection of copyright is not the most effective way of spurring innovation and human creativity. More open approaches, based on encouraging people to share build on existing knowledge and ideas, can also generate business income. For example, this could be through selling training and back up support for open source software, providing hardware and software solutions for businesses, or through selling advertising on websites offering free information and cultural materials. In the case of the music industry, evidence suggests that people who share music online actually purchase more music than other people (BI Norwegian School of Management, quoted in Asay, 2009). Criminalising these people and restricting their internet access may inadvertently have a negative effect on music sales.
Box 7: Alternatives to traditional copyright enforcement

Free and Open Source Software. FOSS is liberally licensed software which allows users to view the source code of the software and hence to easily use, study, change and improve its design. This can help to enhance bottom-up innovation and empower users to tailor applications to meet their specific needs. For example, it is not always commercially viable for software companies to develop software in minority languages. However, open source software allows users to adapt the design to run in other languages themselves, without having to rely on large international companies. The Free Software Foundation and the Open Source Initiative are two examples of groups seeking to promote the use of open software. Linux, Mozilla Firefox, Netscape and Apache are some of the more famous examples of FOSS products.

Creative Commons. Just as the FOSS movement has developed liberal licences for software, liberal licences for content have also been developed, the most famous being the Creative Commons (CC) license. CC licences are part of the open content movement, which sees every user as a potential creator. They allow non-commercial copying and sharing of work provided that the author is given attribution. There are a variety of licences which the copyright-holder can choose from depending on how open they want the content to be.

“Open Access” Movement. This is an academic social movement dedicated to the principle of sharing information. The movement predates the digital age but was galvanised by the potential of the internet in distributing academic journals widely and cheaply. The rationale for the work of this movement can be seen in the opening words of the 2002 Budapest Open Access Initiative Statement: “[a]n old tradition and a new technology have converged to make possible an unprecedented public good. The old tradition is the willingness of scientists and scholars to publish the fruits of their research in scholarly journals without payment, for the sake of inquiry and knowledge. The new technology is the Internet”. To date 5215 individuals and 532 organizations have signed up. An example of this work in practice is AIM laboratory at the University of Cape Town, South Africa which provides assistance to other African universities in developing open access platforms from which to share academic material (Armstrong and Ford, 2006:17).

Efforts to support developing countries to make use of flexibilities. While work is ongoing on the Development Agenda at WIPO, other bodies have also stepped in to encourage developing and developed countries to make use of the flexibilities contained within the international legal regime to broaden access to knowledge. Two notable examples are Consumer International’s 2006 study on copyright and access to knowledge which made policy recommendations (particularly aimed at developing countries) for maximising usage of flexibilities in copyright laws. Another example is the Commonwealth of Learning, an inter-governmental organisation of Commonwealth member states which in May 2004 developed the Document for Commonwealth Countries on Copyright Matters in Education which advocated using flexibilities to their maximum potential within the education sector (Armstrong and Ford, 2006:15).

4.4 Conclusions

The human rights framework recognises the benefits that innovation, creativity and scientific progress can yield for individuals, societies and humanity. ICTs have helped to open up new opportunities for enhancing these benefits and enabling more people across the world to enjoy them. The challenge for the international development, human rights and business communities is to build on these opportunities to develop innovative and flexible business models that spur both human creativity and access to knowledge. However, national and international policy trends are pulling in the opposite direction. The tendency is to enhance intellectual property rights in ways that disproportionately
protect the interests of big business and that threaten to undermine the careful balance between private and public rights to benefit from the production and distribution of culture and knowledge.

Europe has an important role to play on the international stage, both in terms of leading by example and in terms of promoting good practice and standards at the international level. This could be done through taking initiative in standard setting bodies and trade negotiations, for example through driving forwards the development agenda at WIPO. From a human rights perspective, Europe should take every measure possible to ensure that the ACTA process is conducted transparently and that the outcomes restore the balance between public and private rights to knowledge and culture, rather than further upsetting it.

The EU should also support and take on board independent research into the advantages and disadvantages of different approaches to copyright protection in order to counteract a general over-reliance on data produced by industry. Academic analysts have heavily criticised reports produced by industry as overemphasising the costs and dangers of copyright infringement (see for example Karaganis, 2010). Despite this, digital rights activists are concerned that members of the European Parliament’s Legal Affairs Committee are set to adopt a report that conflates online file sharing with trading in counterfeit goods, and that advocates for the criminalisation of intellectual property infringement (EDRi, 2010). Similarly, the Council of Ministers have recently urged the European Commission to revise controversial plans to harmonise the criminalisation of IP infringement across Europe (Council of the EU, 2010b). Such debates need to be based on independent, accurate evidence and consideration of human rights.

In summary, the insertion of human rights principles and standards into these areas by the European Parliament and Commission would help to level the playing field between developed and developing nations in international trade relations; spur innovation and support small business; promote grassroots culture; and enhance human rights to expression and knowledge for people across the world.

5 DIGITAL COMMUNICATIONS AS TOOLS AND EMPOWERING SPACES FOR DEVELOPMENT

Academic and policy discussions about the relationship between human rights and ICTs tend to focus on civil and political rights, with a particular focus on freedom of expression and privacy. However, the evolution of ICTs is also impacting significantly on opportunities for enabling, promoting and protecting economic, social and cultural (ESC) rights. Chapter 4 discussed the impact that ICTs are having on the cultural rights contained in Article 15 of the ICESCR, highlighting the importance of balancing intellectual property rights with rights to participate in cultural life and enjoy the benefits of scientific progress. The role that ICTs are playing in expanding access to information and knowledge has also been discussed throughout this paper, including the ways in which this is helping to bolster and contribute towards the realisation of the right to education contained in Article 13 of the ICESCR.

This chapter builds on this discussion, exploring the potential for ICTs to contribute to the realisation of economic and social rights that are believed to constitute the right to development. These include rights to food, water, work, housing and social services that are essential for physical survival and human development.

ICTs can impact on opportunities for realising economic, social and cultural rights in two main ways. Firstly, ICTs can be instrumental for achieving economic and social rights, providing tools for individuals and/or the state to improve access to monetary income, social goods and public services. For example, mobile banking systems have improved access to credit and systems for transferring money for people
with low incomes across the world. E-governance systems are helping to improve access to public services amongst remote and marginalised communities, including for example making it easier for people to register for public benefits. Secondly, ICTs also have more indirect impacts on society, economy and culture which can have positive effects on economic and social rights. This occurs largely through improving flows of information. This in turn yields economic benefits such as facilitating commerce and trade; social benefits such as improving access to information that empowers citizens to hold governments accountable and to claim their rights; and cultural benefits such as facilitating cultural exchange between communities. This chapter explores these two broad categories in more depth.

5.1 The instrumental impact of ICTs on economic and social rights

ICTs can be used to contribute directly to the realisation of economic and social rights in two main ways. Firstly, at the individual and community level, hardware and software can be developed to provide people with tools to help them improve their quality and standard of living. Secondly, at the community and state levels, ICTS can help to improve public services and social security systems such as health and education.

The rapid spread of mobile phones in developing countries from the end of the 1990s raised awareness within the international development community of the potential for ICTs to help achieve international development goals, including economic and social rights (Souter, 2009b:165). The most widely cited example of the contribution that mobile phones can make to economic empowerment in poor communities is mobile banking (m-banking) and transfer services, such as the popular M-Pesa service in Kenya. Approximately 90% of the world's population does not use formal banking services (Spence and Smith, 2009), whereas mobile phone penetration in developing countries is estimated to have now reached 57 per 100 inhabitants and is continuing to grow (ITU, 2010:1). Whilst access to m-banking services should in theory help to minimise financial risks, help facilitate entry to the formal economy and provide access to financial services and credit for the poor, in reality users have tended to be higher income, urban populations (Bangens and Soderberg, 2008; Alampay and Bala, 2009). This is related to poorer communities relying on irregular incomes, living in cash-based economies and earning too little to make regular savings.

Where m-banking services are used by people at the "bottom of the pyramid" (BOP), it is usually to move or transfer money, rather than to use other banking services (Bangens and Soderberg, 2008). For example, research in the Philippines found that only 1% of people at the BOP had used their mobile phone for banking, and 5% has used it to send or receive money. Research suggests that the main barriers to m-banking and transfer service expansion in many developing countries lie in the regulatory framework and in competition levels within the telecommunications and banking sectors. At the user end, barriers include a lack of understanding of the services and a mismatch between user needs and services offered. If these barriers are overcome, m-banking can be a powerful tool for fighting poverty through lowering the cost of financial transfers and remittances, and for accessing microcredit systems (see for example Diniz et al., 2008; Bangens and Soderberg, 2009).

Mobile banking and microcredit initiatives are not the only way in which ICTs can help to facilitate the realisation of economic and social rights. Thousands of ICT4D initiatives across the world are providing services to poor and remote communities. For example:

- Community telecentres across the world provide rural communities with access to information and communication tools, for example providing access to ICT workshops and remote training courses in rural Mali and Colombia (APCNews, 2009).
− A Dutch NGO Text to Change is helping to communicate knowledge about HIV/AIDS via mobile phones to over 60,000 people in Uganda through interactive text messages (ICT for Development, 2008).
− In Bangladesh, the Palliathya helpline project provides access to virtually any information that they need via women who visit rural households with mobile phones through which they can dial a central help and information centre (Kelly, 2009).
− In Ghana, the "Text Me! flash Me!" Helpline allows phone users to "flash" help centres to signal that they would like to be phoned back by an HIV councillor (ICT for Development, 2010).
− The Jalin Merapi Project in central Java, Indonesia connects community radios, an interactive website and SMS reporting to provide communities living in the vicinity of the Merapi volcano with an early warning system in the case of volcanic activity (2007).
− Mobile Active is a network of NGOs, activists and service providers who are dedicated to using mobile technology for social change (see http://mobileactive.org).

ICTs are also increasingly being used to improve public services such as health and education across the developing world. There has been a shift over the past decade from small scale, donor-funded pilot projects towards larger scale integration of ICTs into public service systems led by national governments and multi-stakeholder initiatives (Farrell and Isaacs, 2007). In the education sector, ICTs have been used to improve the quality and access to teacher training, to enhance learning through interactive teaching materials, and to improve management and administration systems (IIID, 2007). In the health sector, ICTs have been used to disseminate public health information, enable remote consultation, diagnosis and treatment, improve collaboration between health workers, support research, strengthen health monitoring systems and improve administrative systems (InfoDev, 2006). The potential for ICTs to help address climate change and reduce carbon emissions has been receiving increasing attention over the past five years (see for example ITU, 2008 and OECD, 2009).

Whilst evidence suggests that ICT projects have helped to improve public service provision and outputs in many instances, there is an emerging consensus within the ICT4D and wider development community that ICTs are not a panacea or silver bullet. Whether ICTs will help to improve public services depends on a host of social, economic, political and cultural factors. For this reason, researchers stress the importance of carefully designing tools and systems according to actual need and current practices, focusing on cases in which there is reasonable expectation that they will be used and be useful (InfoDev, 2006; Duncombe, 2006).

5.2 Building capabilities through ICTS

As well as directly providing tools and systems for enhancing the realisation of economic and social rights, ICTs can have more indirect effects through improving the capacity of individuals and communities to realise their rights and/or claim them from the state. This line of argument follows Sen's capability approach in which freedom and development are defined by people's abilities to realise their own potential and achieve their personal goals (see Sen, 1999).

ICTs can help to build capabilities and enhance freedoms on a number of levels (Spence and Smith, 2009). In the economic sphere, access to ICTs can help people experiencing poverty to gain access to, or improve, financial income. At the microeconomic level, a range of anecdotal evidence cites cases in which farmers and fishermen use mobile phones to check the price that intermediaries are willing to pay

18 A term used to describe the practice of sending greetings or requesting phone calls through calling a number but then hanging up before the recipient answers. The practice is common amongst lower income phone users who do not have much credit on their phones, and/or when calls are expensive.
pay for their produce, thereby enabling them to go to the buyer offering the highest prices. For example, TradeNet in Ghana provides farmers with information about agricultural markets (World Bank, quoted in Kelly, 2009). In many instances, mobile phones themselves, bought through microcredit, have helped to provide people, in particular women, with a source of income through charging fellow community members for access to the phone. ICTs can help to facilitate entrepreneurialism, putting small businesses into better contact with their suppliers and customers, providing tools for marketing and even platforms for e-commerce. Research suggests, for example, that mobile phones contribute to higher levels of productivity, and can boost GDP by over 5% (Deloitte, quoted in Kelly, 2009).

At the macroeconomic level, ICTs can help to contribute towards economic growth. Many regions and countries that have built industrial policy around ICT manufacture and services have succeeded in boosting investment and trade revenue. Research by Ovum suggests that the mobile phone industry in India has created around 3.6 million jobs (quoted in Kelly, 2009). The rapid growth of mobile phone markets has helped to boost tax revenues in many developing countries (GSM Association, quoted in Kelly, 2009). Macroeconomic growth and increased state revenue should not only provide access to business opportunities and employment, but in theory should also help to increase the capacity of states to realise the economic and social rights of their citizens through improving public service provision and social security. However, it is important not to overemphasise the contribution that investment in the ICT industry and related services can have on economic development. The spur that investment has given to growth in South Korea, Bangalore and Hyderabad has not been widely repeated, largely because growth also requires additional capacities such as an educated workforce, careful management of development strategies and a regulatory and social environment that encourages innovation and entrepreneurship (Souter, 2009c).

In the social and political sphere, digital communications can help to empower individuals and communities through giving them access to the knowledge and tools that they need to hold power holders to account. Amartya Sen famously argued that there has never been a famine in a country with a free press (Dreze and Sen, 1989). Through enhancing information flows and democratising communication, it can be argued that ICTs have the potential to strengthen this effect. Initiatives have arisen across the world that use ICTs to monitor the behaviour of politicians, for example through recording and publicising the attendance and voting behaviour of members of parliament, keeping records of parliamentary and government activity and through monitoring corruption amongst public officials. Mzalendo.com in Kenya is one example. The use of mobile phone cameras and instant messaging to monitor and publicise election fraud has been recorded in a number of countries, including Nigeria, Iraq, Ghana and Sierra Leone. Through improving capacities to access information and speak in the public domain, ICTs are helping to raise awareness amongst people about their rights and providing them with tools to claim them from the state.

5.3 Spurring development and human rights through ICTs: lessons learnt

ICTs have the potential to contribute towards the realisation of economic and social rights, both through providing tools, applications and systems to support rights, and through empowering people to strengthen and claim their rights. However, the evidence base regarding the contribution that ICTs make to the realisation of economic and social rights and other development goals is weak. Research and discourse has tended to focus on the potential of mobile applications to contribute to development, rather than on actual usage, benefits and factors affecting demand and uptake (Kelly, 2009). Moreover, many ICT4D projects have in the past been over-ambitious, with unrealistic expectations of what could be achieved. This has in part been related to a lack of sensitivity to existing communication practices and information needs amongst intended beneficiaries, with the roll out of technologies and tools that are poorly suited to local context.
As a result of these factors, enthusiasm for ICT4D projects has waned amongst donors over the past five to ten years (Souter, 2009c). ICTs are now generally considered as tool for achieving development outcomes such as the Millennium Development Goals rather than as ends in themselves, and are mainstreamed within development programming rather than being the subject of dedicated programmes. This is unfortunate. Declining funding available for ICT4D projects threatens to undermine opportunities for innovative projects with the potential to greatly improve the living standards and capabilities of some of the world's poorest people. It is true that ICTs are not a silver bullet for development. However, rather than dismissing their potential, the international community should draw on lessons learnt over the past decade to build innovative programmes that have significant and sustainable impact.

Firstly, states should have a clear understanding of their responsibility to put measures in place that will spur the realisation of economic and social rights to the maximum of their available resources, as stated in Article 2 of the ICESCR. In relation to ICTs, this responsibility is threefold (Greenstein and Esterhuysen, 2006). Firstly, states should create enabling environments that enable people to drive development themselves. Secondly, they should provide basic public services and infrastructure to support development. Finally, they should not undermine the ability of other states to work towards the realisation of human rights through trade policy or international relations, and should promote international cooperation to build public interest communications networks at local and international levels. To fulfil these responsibilities, ICT policies and strategies need to be developed at national and international levels. These should be publicly owned, based on consultation with poor and marginalised groups, flexible and responsive to changing needs and technologies, and integrated with wider development and human rights strategies.

Secondly, the impact that ICTs have on social, economic and cultural dynamics is highly context specific. Studies of the uptake of mobile banking services demonstrate the important role that regulatory frameworks and market competitiveness have on the nature of services available and their attractiveness to users. Services and systems have to meet clearly identified needs within target communities, and should be accessible and easy to use.

Thirdly, it is impossible to predict what creative solutions technology users will come up with when they have the capacity and tools with which to innovate. Building the capacity of poor communities to empower themselves through ICTs is key. The focus of development programming in this area should therefore be on creating enabling environments that encourage locally owned, needs-based innovation. This will require action at a number of different levels. At national, regional and international levels, internet governance processes and systems should be transparent and participatory to ensure that possibilities to shape the evolution of digital communications are open to marginalised groups. A level playing field for trade, innovation and development is needed at the international level, for example with the abolition of restrictive licensing agreements that limit the use of hardware and software to wealthy sections of society. Policies should encourage the use and spread of open source hardware and software, coupled with capacity building to use, maintain and develop them. Technology users are freer to innovate using open source platforms, for example allowing them to develop applications to meet local needs or to translate software into local languages. Building communications literacy is also crucial, helping people to understand how to use and exploit digital communications systems for personal and community benefit.
5.4 The Challenge of Persistent Digital Divides

The potential for ICTs to deliver development is hampered by the persistent digital divide. The digital divide refers to the gap between those with regular, effective access to digital technologies, in particular the internet, and those without. Internet penetration is uneven nationally and internationally, with cost and insufficient infrastructure acting as significant barriers for many people. Regional differences in internet usage are highlighted in the table below (from UNESCO, 2009:47):

<table>
<thead>
<tr>
<th>Region</th>
<th>Population</th>
<th>Internet users at the end of 2000</th>
<th>Internet users in September 2009</th>
<th>Penetration (users/100 person)</th>
<th>Global ratio (percentage of total number of users)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Africa</td>
<td>991 002 224</td>
<td>4 514 400</td>
<td>67 371 700</td>
<td>6.8%</td>
<td>3.9%</td>
</tr>
<tr>
<td>Asia</td>
<td>3 808 070 503</td>
<td>114 304 000</td>
<td>738 257 230</td>
<td>19.4%</td>
<td>42.6%</td>
</tr>
<tr>
<td>Europe</td>
<td>803 850 858</td>
<td>105 096 093</td>
<td>418 029 796</td>
<td>52%</td>
<td>24.1%</td>
</tr>
<tr>
<td>Near-East</td>
<td>202 687 005</td>
<td>3 284 800</td>
<td>57 425 046</td>
<td>28.3%</td>
<td>3.3%</td>
</tr>
<tr>
<td>North-America</td>
<td>340 831 831</td>
<td>108 096 800</td>
<td>252 908 000</td>
<td>74.2%</td>
<td>14.6%</td>
</tr>
<tr>
<td>Latin-America/Caribbean</td>
<td>586 662 468</td>
<td>18 068 919</td>
<td>179 031 479</td>
<td>30.5%</td>
<td>10.3%</td>
</tr>
<tr>
<td>Oceania</td>
<td>34 700 201</td>
<td>7 620 480</td>
<td>20 970 490</td>
<td>60.4%</td>
<td>1.2%</td>
</tr>
<tr>
<td>World</td>
<td>676 780 190</td>
<td>360 985 492</td>
<td>1 733 993 741</td>
<td>25.6%</td>
<td>100%</td>
</tr>
</tbody>
</table>

At the end of 2009 internet penetration was 64% in developed countries and only 18% in developing countries (only 14% if China is excluded) (ITU, 2010). There are also wide intra-regional disparities, for example with over half of internet users in Africa coming from just five countries (Egypt, Morocco, Algeria, Tunisia and Sudan) (UNESCO, 2009, 49). At the national level internet usage is concentrated in urban rather than rural areas, this is true in both developed and developing countries (see e.g. Economist Intelligence Unit 2008 and Furuholt & Kristiansen, 2007). Digital divides also persist along social lines, reflecting inequality and discrimination against minority groups. This is discussed in relation to women and people with disabilities in Chapter 6.

Many factors contribute to disparities in internet usage, for example lack of content in local languages or lack of electricity. The two most prominent contributing factors are price and accessibility. While broadband prices have dropped sharply over the past few years, in some regions it remains prohibitively high for example in Africa on average a broadband connection costs 500% of the average monthly GNI per capita (ITU, 2010). Access to the internet is generally lower in remote and isolated locations because they are not attractive to service providers due to low rural income levels and/or the high costs involved in providing access (Muente-Kunigami and Navas-Sabater, 2009:3).

5.5 Conclusions

Digital communications have significant potential to contribute to international development, both through providing new tools to achieve development goals and through providing new spaces and opportunities for innovation, empowerment and accountability. Europe should take the lead in integrating ICTs into development cooperation, including supporting the roll out of communications networks in developing countries. The focus should be on eradicating international and local digital divides in access. As the digital communications platform with the widest global reach, particular attention should be paid to opportunities for harnessing mobile phone technologies and applications for development.

Rather than exporting technology and knowhow from the global north to south, the focus of policy in this area should be on empowering poor communities and individuals to develop networks, systems, applications and content that support their needs, whether improving health care or supporting small business. This is likely to require action at national and local levels, for example supporting both the development of progressive ICT policies at national levels and community access and empowerment.
initiatives at local levels. It may also require emphasis on particular technologies and platforms, such as open source hardware and software, and on capacity building for the authoring of relevant content in local languages. Finally, it will require better integration of development policy across different thematic areas. The development of digital communications should both support, and be supported by, policy in other areas such as commerce, trade, education, employment and, not least, human rights.

6 INEQUALITY: A CROSS-CUTTING THREAT TO HUMAN RIGHTS ONLINE

The principle of non-discrimination in the protection and enjoyment of human rights underpins the international human rights framework. The principle is enshrined in Article 2 of the Universal Declaration which states that everyone is entitled to rights “without distinction of any kind such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status”. The principle is reaffirmed in the ICCPR and the ICESCR, and further elaborated in international treaties and conventions such as the Convention on the Elimination of All Forms of Discrimination Against Women, the Convention on the Rights of the Child, the Convention on the Elimination of All Forms of Racial Discrimination and the Convention on the Rights of Persons with Disabilities.

Ensuring equal access to ICTs to all who want it is one of the main issue areas in which the principle of non-discrimination is commonly applied to ICTs. The internet is increasingly seen as a public good or service within international and national policy arenas. When services are provided for the general public, providers should ensure equal access for all, without discrimination on personal or political grounds (Zarrehparvar, 2006). There has been much debate in recent years as to whether internet access itself is a fundamental human right. For example, the passage of the EU Telecoms Reform Package was delayed in 2009 by disagreement as to whether states should be permitted to mandate ISPs to cut the internet access of customers suspected of illegal downloading on the grounds that internet access is a fundamental right. The final Package stops short of defining internet access itself as a right. However, it does contain an “internet freedom provision” which recognises the fundamental importance of internet access19, and which the European Parliament has argued effectively gives it the same legal protections as a fundamental right (European Parliament, 2009a). Internet access has been declared to be a human right in Estonia and France, and 1mb broadband access is a legal right in Finland. A recent survey conducted in 26 countries around the world found that 79% of respondents believed that internet access should be a fundamental right (BBC News, 2010c).

The internet is thus increasingly recognised as an essential public good, instrumental for the full realisation of human rights, if not a fundamental right in itself. It is therefore important that states apply the principle of non discrimination to the internet, ensuring that all people are able to enjoy the benefits that it brings. However, a significant proportion of the world’s population currently does not have access to the internet and other digital communication platforms due to a lack of access to

---

19 The provision states that “Measures taken by Member States regarding end-users’ access to or use of services and applications through electronic communications networks shall respect the fundamental rights and freedoms of natural persons”. It also states that any restrictions on access must be appropriate, proportionate and necessary within a democratic society, with "effective judicial review and due process".
physical infrastructure, insufficient financial resources, illiteracy, disability and gender discrimination. It can also be argued that the ICT environment itself is inherently discriminatory as large sections of the population are excluded from its design, management and governance. Internet and communications innovation and policy is on the whole dominated by middle class males, meaning that it is shaped predominantly according to their needs and wishes rather than those of other actual and potential internet user groups. This presents the danger of ICTs being used to maintain and even exacerbate current patterns of inequality rather than battle against them, for example with surveillance mechanisms being used to control the behaviour of minority groups online or electronic communications facilitating the trafficking of women.

This chapter explores these issues in greater depth through focusing on two significant categories of discrimination that have been deeply affected by the evolution of ICTs: gender and disability. Europe has an important role to play in pushing for equality in people’s ability to shape, access and use digital communications. Indeed, through ratifying the UN Convention on the Rights of Persons with Disabilities, the EU has committed itself to pursuing equality for people with disability both within the EU and through its foreign relations and development cooperation. These commitments should be taken seriously. Global digital communications environments must support the human rights of all individuals; not simply those who currently have the power to make themselves heard in communications policy spaces.

6.1 Pursuing gender equality in and through ICTs

The important role that the media and communications have to play in the global battle for gender equality is recognised in the Nairobi Forward-looking Strategies of the Advancement of Women, adopted at the UN Third World Conference on Women in 1985. It is further elaborated in Section J of the Beijing Platform for Action, adopted at the Fourth World Conference in 1995. This sets two strategic objectives for governments, media organisations and professional associations:

- Increase the participation and access of women to expression and decision-making in and through the media and new technologies of communication.
- Promote a balanced and non-stereotyped portrayal of women in the media.

The Nairobi and Beijing conferences put ICTs on the issue agenda of the global women’s movement (Jensen, 2006). The outcome documents from the conference stress the important role that offline and digital media play in shaping societal values and norms, and also their potential for empowering women. They therefore call not only for the regulation of media content, but also for the participation of women in media production, management and governance.

However, gender and ICT activists have been disappointed by the lack of attention that has been paid to Section J of the Platform for Action since 1995 (see for example Kee, 2005 & 2010). Within both the international women’s movement and the international development community, ICTs are increasingly seen as tools that can be used to exacerbate or tackle gender issues directly, rather than as part of communications spaces that embody and reproduce gender inequality. For example, sessions at recent women’s rights conferences have focused on the potential of ICTs to enhance communication about gender issues and networking amongst women (Jensen, 2010). The scant reference to ICTs within the MDG framework has led to a focus on using ICTs to achieve development goals such as maternal and child health, rather than on developing media and communications environments that challenge societal norms and give women equal control over both public discourse and the direction of

20 See Chapter 5.4 for a discussion of digital divides at international and local levels, with a focus on disparities caused by income and geography.
technological innovation (Jensen, 2006). Indeed there is no mention of technologies in the EU Development Policy on Gender Equality (European Commission, 2007).

Whilst ICTs do provide important new opportunities, platforms and tools for directly fighting against the violation of women’s rights, it is imperative to address the role that digital communications are playing in reflecting and reinforcing inequality between men and women at local, national and international levels. Five main issues deserve particular attention.

First is the issue of access to ICTs. Gender divides in access and use of ICTs are pervasive in many countries around the world. Whilst evidence suggests that these divides are more significant in developing countries, men also represent a much higher proportion of internet users in a large number of countries in the global north, including the UK, Germany and Greece (Hafkin and Huyer, 2007). In many of the world’s poorest countries, rates of poverty, illiteracy, education and formal employment are lower among women than men, giving them lower levels of access to ICTs (Jensen, 2006). A 2006 study of ICT access and use in six francophone countries in West Africa found that women on average have 35% fewer opportunities and benefits yielding from ICTs than men, based on a composite indicator encompassing different dimensions of gender disparity (Gender and ICT Network, cited in Hafkin and Huyer, 2007). Disparities in the capacity to use ICTs were higher than in physical access, highlighting the importance of taking into account factors that indirectly affect ICT access when developing ICT policy and strategy.

Policy and action in these areas is hampered by a paucity of data and analysis, with very little national level data concerning ICT access and use being disaggregated by gender (Zarrehparvar, 2006; Hafkin and Huyer, 2007). However, even if disaggregated statistics were available, they would reveal little about the factors that contribute towards gender-based digital divides, which are often rooted in underlying power inequalities and socio-cultural norms. For example, in societies that allow women very little visibility in public, access to the internet via internet cafes is effectively restricted to men (Zarrehparvar, 2006). Access to ICTs in the private domain tends to be controlled by men in a number of countries, for example with men limiting or restricting access to phones and the internet in households in Pakistan and Uganda (Randhawa, 2010; Madanda et al., 2009).

The second main issue area relates to access to, and creation of, communications content and information. Men have historically dominated the arena of public communications throughout the world, determining what is considered to be legitimate and relevant information for the public domain. Jensen (2006) highlights how this continues across the world, exacerbated by the dominance of men in decision making professions such as government, news making and scientific research. This effectively distorts the public sphere of information and ideas, marginalising opinions and knowledge created by and for women. ICT4D programmes have frequently been criticised for making assumptions about the kinds of tools and information that people within communities they are targeting want and need (Duncombe, 2006). An evaluation of telecentre projects in Uganda found that, whilst men tended to search for information on politics, economics and business, women came to find information about a range of different subjects such as health, education, training and setting up small businesses (Etta, 2003). Owing to a lack of disaggregated content and low levels of media literacy, women were often unable to find the information they were looking for, and tended not to return to the telecentres. There is an urgent need for the production of relevant, local content that meets the information needs of marginalised women, preferably through empowering them to communicate in the public domain themselves (Jensen, 2006).

The third issue concerns the civil and political rights of women online, particularly freedom of expression and privacy. Malhotra (2007) highlights how laws and regulation determining what is deemed to be acceptable public content in many countries date back to colonial times, with
interpretation continuing to be influenced by social, political and cultural norms that discriminate against women. Such "obscenity laws" either directly censor or effectively stifle personal expression about a range of issues, particularly relating to sexuality, and can also have public health implications, for example limiting access to sexual and reproductive health information.

ICTs have opened up new spaces for women to express themselves and communicate in the private and public domains, for example with social networking sites providing young people in the Middle East with opportunities to interact with the opposite sex, and bulletin boards providing women with opportunities to express their opinions in ways that would not be acceptable in the offline public sphere (Al-Saggaf, 2006). However, ICTs also offer new opportunities for monitoring and control, with women leaving "trails of digital data" behind them which can undermine the empowering effects that access to digital communications might have (Jensen, 2006). Monitoring conversations in internet chat rooms, stalking on social networking sites, intercepting emails and tracing internet activity through web browser histories are just some of the ways in which ICTs lend extra power to perpetrators of violence against women (Kee, 2005). Less obvious violations of women's privacy have also been revealed in a number of contexts, for example with reports of sim card vendors in Pakistan selling personal details of female customers to male customers, including their phone numbers and personal descriptions, thereby acting as unauthorised dating services (Kee, 2010).

The final, cross-cutting issue is the under-representation of women in the media and ICT industries and governance bodies. This is dangerous on a number of levels. At all "layers" of the communications environment, women are missing out on opportunities to shape the nature, content and possibilities of communication. Issues include the portrayal of women and gender issues; the selection and portrayal of public policy issues; and the design of digital communication tools, the perceived needs that they meet and the uses to which they are permitted to be put. Public communications via the media have always played a very powerful role in society, helping to shape public norms and political debate. ICTs are increasing the power of communication through increasing the pervasiveness and role of information and communication in all aspects of social, economic and political life. They are also opening up new opportunities for social advancement and, as this paper has shown, prospects for protecting and advancing human rights. It is therefore all the more important that women and men have equal opportunities to participate in and shape digital communication environments to meet their wants and needs. Otherwise, patterns of gender discrimination and inequality will be exacerbated; reinforced by and reflected in the information society.

6.2 Ensuring equal access for persons with disabilities

ICTs have dramatically increased opportunities for the realisation of the human rights of people living with disabilities. Physical barriers to accessing information are being broken down, with resources increasingly available in the home via the internet. ICT tools can help to provide access to communications content in new ways, for example with automated text readers providing access to written material for people with visual impairment. ICTs are also expanding opportunities for people with disabilities to participate more actively in society and in community life, and help to improve employment opportunities (W3C, 2009).

The UN Convention on the Rights of Persons with Disabilities (CRPD) explicitly refers to the rights of all people to accessible ICTs. Article 9 of the Convention refers to accessibility, stating, "to enable persons with disabilities to live independently and participate fully in all aspects of life, States Parties shall take appropriate measures to ensure to persons with disabilities access, on an equal basis with others, to the physical environment, to transportation, to information and communications, including information and communications technologies and systems, and to other facilities and services open or provided to the public, both in urban and in rural areas." Article 9(2) requires states to take appropriate measures to
"Promote access for persons with disabilities to new information and communications technologies and systems, including the Internet" and "promote the design, development, production and distribution of accessible information and communications technologies and systems at an early stage, so that these technologies and systems become accessible at minimum cost." Article 21 requires that states ensure persons with disability are able to exercise their right to freedom of expression, including by ensuring that public information is available via accessible formats and technologies and by encouraging private service providers and the media to do the same, including on the internet.

The European Union signed the CRPD on March 30, 2007, as the first core human rights treaty to be signed by European Community this was a historic step so should have a significant impact of EU foreign policy. Article 32 of the Convention calls for international cooperation to support the realization of the rights of persons with disabilities; measures could include “facilitating and supporting capacity-building” and “facilitating access to and sharing of accessible and assistive technologies, and through the transfer of technologies”.

Technologies that help to improve accessibility and usability to and on the internet have improved rapidly over the past decade, not least because of the standardisation of protocols and technologies led by organisations such as the ITU and the W3C. Examples of the technologies available are outlined in Box 8. However, despite improvements in technology, the proportion of internet content that is fully accessible to all people with disabilities is extremely limited. This is largely because most web developers do not use protocols or follow guidelines that enable standardised tools to make content accessible to users with different disabilities. For example, people who find it difficult to use a mouse cannot use sites that require mouse interaction, and people who are blind are unable to interpret visual images if web developers do not provide textual interpretations to describe them (W3C, 2009). A 2006 UN-commissioned study of websites in 20 countries found that 98% of websites tested did not adhere to programming standards that allow for full accessibility for people with disabilities (Nomensa, cited in Information Week, 2006).

Box 8: Assistive technologies to improve the accessibility and usability of the internet

- Refreshable Braille: portable mechanical displays that allow pins to be raised and lowered dynamically so that electronic text can be read by people who are blind.
- Scanning software: programmes that highlight or read out menu items or links for people with physical or cognitive disabilities, allowing users to push a switch to select the desired item.
- Screen magnifiers: software that magnifies portions of computer screens for people with low vision.
- Screen readers: software that translates content into audio outputs or refreshable Braille for people who are blind or dyslexic.
- Speech recognition: software that allows people to input information and data vocally.
- Voice browsers: systems that allow for voice-driven navigation of the internet.
- Alternative keyboards or switches: these provide alternatives for people who have difficulties using standard keyboards and mice.

Source: W3C working draft: How People with Disabilities Use the Web. (A final version of this paper is due to be published in 2010.)

---

21 Argentina, Australia, Brazil, Canada, Chile, China, France, Germany, India, Japan, Kenya, Mexico, Morocco, Russia, Singapore, South Africa, Spain, United Arab Emirates, the United Kingdom and the United States
Other barriers that limit accessibility for people with disabilities include prohibitive costs of assistive technologies such as Braille keyboards, a lack of training and education to use ICTs and assistive technologies, and socio-cultural environments that do not encourage internet use (W3C, 2009). These factors combine to result in lower levels of access to and use of ICTs amongst people with disabilities than amongst people without disabilities. In the US, recent research has found that the percentage of people with disabilities who have access to broadband at home is two thirds of the national average (Horrigan, 2010). The same study found that elderly people with disabilities were 75% less likely to have access to broadband than those without disabilities.

Whilst there is a lack of statistics available for access amongst people with disabilities in developing countries, it can be assumed that accessibility figures are even lower owing to lower financial income, higher levels of poverty, and poorer protection of the rights of people with disabilities. A study of website accessibility across UN member countries found that those with higher percentages of accessible websites have higher levels of public and individual investment in ICT, stronger protections for equality in society and a higher percentage of urban population (Thompson et al., 2007). There is an urgent need for a stronger focus on ensuring equal accessibility for all within ICT4D strategies and interventions.

6.3 Conclusions

Digital communications environments are not apolitical spaces. The same power relationships and inequalities that pervade in the offline world also affect people’s use of ICTs and their experiences online. ICTs can be used as tools to help empower minorities and groups that are discriminated against. However, they can also be used as tools of discrimination themselves through permitting targeting surveillance and censorship. Digital communication environments can also embody and reproduce inequality, with persistent differentials in levels of access to ICTs, participation in their governance, ability to influence directions of innovation, and capacities to produce and access content.

Through its foreign relations and its participation in multilateral policy fora, the EU could help to raise awareness about the importance of building non-discriminatory and inclusive digital communications environments at national and international levels. This chapter has focused on gender equality and the rights of people with disabilities. However, the issues raised affect a range of different minority groups across the world. In some instances, discrimination is more obvious, for example with sites concerning lesbian, gay and transsexual rights being a common target of internet filtering. In other instances, discrimination is less obvious, with national level data concerning access to ICTs hiding regional digital divides and providing few insights into the actual capacity of people to use ICTs in a meaningful way. Equality issues therefore need to be considered in all aspects of ICT work, with explicit attention given to understanding the needs of different groups and anticipating the ways in which policy is likely to affect them.

7 POLICY AND PRACTICE OPTIONS FOR THE EU

As a powerful actor on the world stage and region with the most advanced human rights institutions, the EU has an important role to play in helping to build digital communications environments that support and expand human rights. There are four main ways in which the EU can influence the capacity of digital communications to support human rights. Firstly, it can influence international standards and practice indirectly through its internal policy. Secondly, it can influence international standards and practice directly through participating in international policy fora. Thirdly, it can use foreign diplomacy to encourage or pressure countries and institutions to uphold human rights. Fourthly, it can support companies and other stakeholders within its jurisdiction to build progressive business models and
online practices that uphold and expand human rights rather than undermining them. This chapter explores these strategies in more depth, examining their effectiveness and the relationships between them.

7.1 Leading by example through internal policy

Much of the work that has been undertaken regarding policy and legislation at the EU level on human rights and ICTs has focused on internal policy issues that are relevant to member states. Internal EU policy and regulation relating to digital communications is not only of relevance to European citizens, but also has significant implications for the capacity of digital communications to support and expand human rights at the global level.

Firstly, the EU is a powerful global political force, and European policy can effectively set standards for policy outside of the EU. The EU therefore has an important role to play in promoting a culture of human rights protection at the international level, including within discussions about ICT policy and governance. Its ability to do so will be severely undermined if its internal policies and practices do not uphold human rights. Moreover, technology that is designed to control digital communications for apparently legitimate reasons can be used by repressive governments to violate human rights. Therefore, it is pertinent to advance positive policies promoting open and free communication and understanding of the issues amongst stakeholders, rather than negative policies which encourage the development of technologies of control and surveillance. Similarly, controlling internet content for legitimate reasons can act as a smokescreen for repressive countries who claim that they are acting in line with global standards, but are in practice censoring and monitoring their citizens for political reasons rather than legitimate aims. The internet is also a global communications medium, and placing restrictions on communication within the EU therefore affects people outside of the region. For example, if EU policies such as “three strikes” laws have chilling effects on information sharing, people outside of the EU who may have benefitted from cultural and information exchange will be affected.

For these reasons, this report has covered a range of issues that affect people both inside and outside of the EU. It has highlighted that there is a need for better coordination on policy issues relating to the internet across all departments of the European Parliament, Commission and Council, with better consideration of strategies for promoting human rights and an open internet throughout. Relevant policy areas identified by this report in which the EU has been active include efforts to promote cyber-security, enhance child protection online and improve the protection of European citizens’ data. From a human rights perspective, EU policy and regulation in these areas is mixed, with the European Parliament frequently criticising the Commission for paying inadequate attention to human rights. There is an urgent need for policy in all of these areas to be reviewed as if the EU is serious about protecting and expanding human rights at the international level. Owing to the convergence of communication around internet technologies, human rights need to be mainstreamed across all policy departments that are responsible for any issues relating to communication at all “layers” of digital communication environments. These include foreign affairs, international development, consumer rights, culture and trade. Too often, the EU’s internal policy has been influenced by moral panic, including over child protection and cyber-security, or by the interests of big business, as in debates concerning copyright protection. The direct and indirect effects that policies have on human rights and on the capacity of evolving digital communications to support rights needs to be taken into consideration better. Any policies which impinge on human rights must meet the strict three part test for imposing limitations on rights, and should always aim to enhance the open and empowering dimensions of the internet.

In light of this, human rights concerns should be mainstreamed throughout the European Commission’s new Digital Agenda for Europe. These efforts should be coordinated with the
implementation of the Grenada Strategy to promote the Information Society in Europe between 2010 and 2015, proposed by the Spanish Presidency of the EU. The strategy includes plans for the creation of a European Charter of Rights of Users of Electronic Communications to reinforce users’ rights in Europe (Spanish Presidency of the EU, 2010a). This is an initiative that the EU should prioritise, ensuring that human rights are secured through the resulting Charter. The IGF Dynamic Coalition on Internet Rights and Principles (see section 7.2b) is currently working on a similar Charter through multi-stakeholder collaboration. Opportunities for coordination between these efforts should be explored.

The European Parliament has on a number of occasions played a positive role in pushing for better respect for human rights within internal EU policy, for example in the passage of the EU telecoms package and in their condemnation of the lack of transparency in the ACTA negotiations. Parliament has also worked proactively on issues. For example, in March 2009 it adopted a resolution on Strengthening security and fundamental freedoms on the internet, presented by the Committee Civil Liberties, Justice and Home Affairs. The resolution calls for a better balancing of security, freedoms and privacy protection on the internet. Some of the resolution’s recommendations are questionable, including those encouraging manufacturers to pre-install child protection software on computers and recommending measures to criminalise the violation of intellectual property rights. However, it is significant that the European Parliament has taken a holistic approach to the issues, and recognises the importance of protecting human rights and fundamental freedoms on the internet. This approach now needs to be applied in practice, with better coordination between relevant parliament committees, and human rights and communication concerns mainstreamed throughout.

7.2 Raising standards in international fora

The EU must advocate for human rights protection within international policy fora. However, the EU has a mixed track record in helping to set international standards to build digital communication environments that support human rights. The EU should work to develop a consistent policy framework for building open and empowering communications environments across the international spheres in which it participates. In other words, human rights need to be explicitly mainstreamed throughout EU policy. The broad policy spheres in which human rights need to be inserted are outlined below.

7.2.1 The World Summit on the Information Society

Following a UN General Assembly resolution, the World Summit on the Information Society (WSIS) was held in two phases in 2003 and 2005 to “take concrete steps to establish the foundations for an Information Society for all, reflecting all the different interests at stake” (WSIS[a]). WSIS played a significant role in raising awareness at the international level about the role that ICTs can play in protecting and expanding human rights. This was largely the result of efforts taken by a number of stakeholders to push for greater consideration of human rights as a cross cutting issue within the information society, and for official texts produced by the Summit to be fully consistent with human rights (Drake and Jorgensen, 2006). The civil society Human Rights Caucus was particularly active during this process (ibid), and the European Commission also played a role (European Parliament, 2008).

Through the WSIS Geneva Declaration of Principles and the Tunis Agenda for the Information Society, the world’s governments reaffirmed their commitment to protecting human rights in the information society, and in particular the right to freedom of expression:

“We…declare our common desire and commitment to build a people-centred, inclusive and development-oriented Information Society…respecting fully and upholding the Universal Declaration of Human Rights” (Article 1, Geneva Principles).
“We reaffirm our commitment to the freedom to seek, receive, impart and use information, in particular, for the creation, accumulation and dissemination of knowledge… We affirm that measures undertaken to ensure Internet stability and security… must protect and respect the provisions for privacy and freedom of expression as contained in the relevant parts of the Universal Declaration of Human Rights and the Geneva Declaration of Principles” (Article 42, Tunis Agenda).

The Geneva Plan of Action (2003) sets up a number of “action lines” designed to facilitate work towards the commitments made in the Geneva Declaration and Tunis Agenda in a range of areas spanning from communications infrastructure, content and use. Overall review of WSIS implementation is the responsibility of the UN Commission on Science and Technology for Development (CSTD). International bodies such as the ITU and UNESCO act as moderators of each action line, and annual facilitation and stock taking meetings are held to gauge progress. Whilst protecting human rights is not a direct or explicit aim of any of the action lines, nearly all lines are relevant for building digital environments that are conducive for the full protection and realisation of human rights.

Despite this, in practice, very little concrete, coordinated action has been taken at the UN level to ensure that the information society respects and upholds human rights. No independent resources have been dedicated to achieving the action lines, and very few new activities have been generated to work towards them (Souter, 2009). WSIS was successful in achieving its aims of raising international awareness about the importance of ICTs in society, and establishing a framework for cooperation (ibid). However, rather than improving coordination, many of the issues that the Summit covered continue to be addressed in the disparate array of national, regional and international institutions that make up the internet governance and ICT for Development (ICT4D) ecosystem. Progress is being made in some areas, but not in others. As the protection and promotion of human rights in and through the information society was not an explicit action line of the WSIS process, it has more or less slipped off the international agenda.

7.2.2 Internet Governance

7.2.2.1 The Internet Governance Forum

The WSIS process established the Internet Governance Forum, an annual gathering that is open to any interested stakeholder from the business, government or civil society sectors. Internet governance has been defined as “the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet” (WGIG, 2005). The mandate of the Forum is to discuss, inter alia, “public policy issues related to key elements of Internet governance”, and to promote and assess the embodiment of WSIS principles in internet governance processes (Tunis Agenda: para 72). The IGF is not a decision making body, but is rather intended to promote dialogue and cooperation between actors and institutions involved in internet governance. It is this characteristic that has led many stakeholders to push for the continuation of the Forum. The Forum initially had a five year mandate which is set to expire in 2010, but is expected to be renewed this year.

Plenary discussions at the IGF have been broadly structured around four main themes: openness, diversity, security and access. Rights issues have tended to have been included in the openness theme. Analysis of changes in the agenda and emphasis of the IGF over its five year mandate reveals diminishing attention to the theme of preserving the openness of the internet as an issue in its own right, and to related themes such as freedom of expression (Horner, 2009). Openness is now generally discussed in relation to balancing it with concerns to promote cyber-security, diminishing the scope for more positive policy-oriented discussions about expanding open spaces for freedom of expression and
cultural exchange on the internet. However, a number of stakeholders have been vocal within the IGF about the importance of upholding human rights in and through internet governance, and there was broad consensus at the 2009 Forum that human rights and security are not binary issues and do not have to be traded off against each other (APC, 2009).

The IGF remains an important arena for raising awareness about the human rights dimensions of ICTs and for fostering cooperation between stakeholders to address pertinent issues. The Forum also houses the Dynamic Coalition on Internet Rights and Principles, an independent multi-stakeholder network of individuals and organisations that is working to raise awareness about rights issues within the Forum and other arenas, and to instigate initiatives to address them\(^\text{22}\). The main challenges now are to enhance cooperation between different stakeholders who are concerned with protecting and advancing human rights, and to help internet governance organisations to mainstream consideration of human rights within governance processes. There is also a need to reach out to new constituencies that are not well represented in current discussions and processes. These include developing countries, minority groups and organisations within the traditional human rights community that have not engaged with ICT issues.

7.2.2.2 Internet governance institutions

The internet is currently governed by a wide range of institutions and actors, each responsible for processes across different geographical, technical and social dimensions. Mathiason et al. (2004) divide internet governance actors into four categories: state institutions with universal membership, including primarily those organisations that are part of or linked with the UN such as the ITU and UNESCO; state institutions with non-universal membership, including for example the OECD and Council of Europe; informal non-State institutions such as the standard setting bodies IETF and W3C; formal non-State institutions such as ICANN; and state actors working bilaterally and at the national level\(^\text{23}\). Internet users themselves, whether business, government, civil society or private individuals, also play a significant role through lobbying or direct participation in governance processes, and through everyday use of the internet which creates norms to guide behaviour and markets for certain products and services.

It is beyond the scope of this paper to examine these institutions and actors in depth. However, it should be noted that the main complaints that civil society and accountability organisations have regarding current internet governance structures revolve around their lack of transparency, public participation and public accountability, as well as their dominance by actors from the Western Hemisphere (see Mathiason et al. (2004) and Mueller (2009) for further discussion). In response, the Council of Europe, Association for Progressive Communications and United Nations Economic Commission for Europe have developed a Code of Participation on Information, Transparency and Participation in Internet Governance\(^\text{24}\).

\(^{22}\) Formerly the Dynamic Coalition on an Internet Bill of Rights.

See \url{http://internetrightsandprinciples.org/}

\(^{23}\) The acronyms used here stand for:

ITU – International Telecommunications Union

UNESCO – United Nations Educational Scientific and Cultural Organisation

OECD – Organisation for Economic Co-operation and Development

IETF – Internet Engineering Taskforce

W3C – World Wide Web Consortium

ICANN – Internet Corporation for Assigned Names and Numbers.

\(^{24}\) See \url{http://www.unece.org/env/pp/related.htm for more information}.
On the whole, there is general agreement that governance structures should remain dispersed, multi-stakeholder and bottom-up, rather than top-down and controlled by governments. Thus, attempts to coordinate governance at the international level in a top down manner tend to be seen as threatening by actors and institutions who have, over the years, built up experience and authority over different aspects of the internet environment. Open discussion and informal networking is therefore currently preferred by a range of stakeholders to granting the IGF, or an alternative body, decision making powers concerning the vast array of issues encompassed by the term “internet governance’. The EU has not played as strong a role in internet governance as it could. It should work with the Council of Europe and others to develop policies and standards for promoting public interest across the institutions and processes that make up the internet governance system, mainstreaming respect for human rights throughout (Kettemann, 2010).

7.2.3 Trade institutions

This report has highlighted the ways in which policy spheres that do not have an obvious relation to communication rights can influence the capacity of digital communications to support human rights, and the direction of their continued evolution. It is therefore important that the EU develops a consistent and coherent policy framework for protecting and expanding human rights across these policy spheres.

Where issues directly relate to human rights and communication, the EU has on a number of occasions been vocal in advocating for the protection and promotion of human rights online. For example, the Commission claims a role in the inclusion of commitments to human rights protection in the official outcome documents of the WSIS (European Parliament, 2008), and has made repeated calls for the protection of an open and inclusive internet at the meetings of the IGF (see Reding, 2009).

However, the EU has played a less positive role in fora in which issues are not explicitly or directly related to human rights, but which still either directly affect rights or the capacity of digital communications to support rights. For example, the EU could do more to promote a human rights agenda within internet governance institutions such as ICANN and the ITU, as well as in trade and copyright institutions such as the WTO and WIPO. Such fora are arguably more important as they directly influence policy and practice, unlike the IGF which is primarily a venue for networking and dialogue.

7.2.4 Human rights institutions

The EU has relations with many international human rights institutions and can use its political power to push for better awareness of, and commitment to human rights standards being implemented on the internet. How different rights apply to the online environment is still not well defined, and the EU could push for more guidance here. Specific actions which the EU might take include sponsoring resolutions on these issues, supporting relevant initiatives from other states, and using informal networks and diplomacy to promote awareness and consensus. The EU can also use its political power to try and resist pressures to dilute human rights standards, such as proposals regarding the defamation of religions.

7.3 Exerting influence through diplomacy

Whilst most EU policy concerning ICTs and human rights at the EU level have focused on internal rather than external affairs, human rights and communication concerns are also addressed within foreign policy. Section 2.3 of this report outlined the diplomatic channels through which the EU has condemned online censorship, drawing on examples from Belarus and Iran.
The EU should continue to monitor human rights abuses that are occurring in and through digital communications environments. Criticism should be strong and consistent, with the EU sending the clear message that human rights abuse online is as serious as it is offline. The focus should not only be on notorious human rights violators; attention needs to be drawn to the increasing pervasiveness of online censorship across the world and the dangers that this presents in terms of damaging the overall openness and empowering capacities of the internet.

However, as discussed in section 2.3c, criticism alone is not enough. In 2009 Swedish Presidency of the EU made freedom of expression on the internet an important area for consideration during their tenure. The EU should continue to make freedom of expression online a priority of foreign policy, building on the policy and dialogue work conducted during the Swedish Presidency. The EU should also exert influence through its trade policy and through multilateral negotiation. It should also bolster these efforts through taking positive action to support stakeholders to actively uphold human rights through their activities and business online. This is discussed below in relation to the corporate sector.

7.4 Supporting ICT stakeholders to uphold and expand human rights

There is emerging consensus within the international internet governance community that, rather than top down legislation, co-regulatory approaches are the most appropriate means of protecting human rights in online environments. Sectors within the online industry have been shown to be innovative in terms of self-regulation, for example with social networking sites tackling child grooming through installing whistle blowing and reporting buttons, and companies voluntarily participating in projects such as the GNI. However, human rights are too important to be left to self-regulation alone. On the other hand, it is essential to maintain the internet as an innovative, creative and empowering space. Multi-layered regulatory approaches are needed, reflecting the dispersed and multi-layered nature of digital networks (Kleinsteuber, 2004).

National and multi-lateral government has an important role to play in supporting businesses to make sound operating decisions and to fulfil their responsibilities to respect human rights. As a recent study into options for internet regulation for the European Commission concluded, there are no magic bullets; continual political judgement and cost benefit analyses are required regarding the efficacy of industry-led approaches and their ability to foster digital communications environments that uphold human rights and the public interest (Cave et al., 2008). Rather than focusing on restrictive top-down legislation, the EU should be providing the policy space, support and resources that are required for effective self-regulation by companies operating in digital environments. The emphasis needs to be on raising awareness about the importance of human rights, on education about what they mean in practice and on encouraging innovative and sustainable solutions. Support should be monitored for effectiveness on an ongoing basis, and adapted according to changing needs and technological, political and economic developments.

The Global Network Initiative (GNI ) has been discussed in this report as one example of a positive, co-regulatory initiative. The GNI is a collaborative effort by companies and civil society organisations to help online companies respect and advance human rights. The Initiative has produced guidelines for companies operating in countries with poor protections for human rights, and has established a Governance, Learning and Accountability Framework to help companies uphold freedom of expression and privacy principles in and through their business. However, company membership of the Initiative is currently limited to Google, Yahoo! and Microsoft. Support from a wider cross section of communications companies is needed to expand its guidelines to make them useful for a wider range of companies (GNI, 2010).

7.5 The Council of Europe
Discussion of initiatives taken by bodies other than the UN and EU is outside of the terms of reference for this report. However, we recommend that the Subcommittee on Human Rights considers the important standard setting initiatives and guidelines that are being undertaken by the Council of Europe (CoE) pertaining to the protection and promotion of human rights on the internet. Whilst some of the CoE’s work has presented serious challenges for the protection of human rights online, most notably the Cybercrime Convention as discussed in this report, it has also issued a number of progressive declarations and recommendations. For example, these include recommendations on promoting freedom of expression with respect to internet filters (CoE, 2008) and on measures to promote the public service value of the internet (CoE, 2007).

The CoE has also worked with the private sector to produce co-regulatory guidelines for human rights protection for ISPs and online games providers (CoE, 2008a&b). The CoE’s Committee of Experts on New Media is currently preparing recommendations on social networking services; on network neutrality; and on whether we need a new notion of “media” in the information age that defines the rights, roles and responsibilities of different stakeholders in order to protect the public service value of communications. The Council of Europe has taken the lead in interpreting and applying human rights standards to digital communications environments, and the EU should incorporate and build on this work within its internal and external policy.

8 CONCLUSIONS AND RECOMMENDATIONS

8.1 Developing positive and enabling policy frameworks

The evolution of ICTs has revolutionised communication and, in doing so, has had significant and wide reaching impact on prospects for protecting and fully realising human rights. This paper has explored the impacts across the spectrum of the human rights framework, looking at civil, political, economic, social and cultural rights. On balance, the assessment is positive. Digital communications are empowering people to express themselves, access knowledge, share culture, advance their well being and participate in society in unprecedented ways. However, a number of dynamics and trends within digital environments are at the same time posing challenges to human rights, threatening to close down the new communication spaces that have emerged. These include the erosion of open communication spaces by efforts to fight cybercrime, the undermining of opportunities to realise rights to culture, knowledge and expression through overzealous copyright protection, and the reproduction and reinforcement of inequality within digital environments. These dynamics are not a direct result of technological change per se. Rather, they are social, political and economic trends and pressures that are shaping the development of communications technology and practice. There is therefore a need to build a positive and enabling policy framework to encourage digital communications to evolve in such a way as to support and expand human rights and the public interest, rather than erode them.

This framework needs to be developed and applied in a consistent manner across a range of different policy areas and across all “layers” of digital communications environments, at national and international levels. Policy spheres that have traditionally been seen as distinct are now converging as digital communications bring together previously separate communication platforms. These spheres include media, telecommunications, data protection, intellectual property, security and science and technology. As demonstrated by this paper, human rights are affected by policy in all of these areas because they all affect human capacitakes to seek, receive, impart and share information, knowledge and culture. We cannot afford to ignore the human rights dimensions of intellectual property trends for example, or of intermediary liability on the internet. There is therefore a need for a consistent policy approach that recognises both the indivisibility of human rights and of digital communications
environments. Owing to the international nature of the internet, the domestic and international elements of these overlapping policy areas also require coordination.

Much disagreement within debates concerning ICT policy appears to stem from confusion over whether the internet is a medium for personal communication or for publishing. In fact, it is both of these things and more. Communication policy needs to appreciate and embrace this complexity. To be effective, the process of fostering positive policy and governance frameworks for digital communications will therefore require the development of new partnerships with people, organisations and companies that have a stake in the environment. Digital communications environments are complex, multi-layered spaces which bring together a wide range of stakeholders who use communications for different purposes, and who therefore have different interests and needs. To ensure that digital environments remain useful and innovative, all of these stakeholders need to be involved in defining appropriate policy frameworks, and where relevant, in maintaining them. Governance and policy processes have to meaningfully involve the technical community, governments, civil society and business, taking into account that these broad categories themselves encompass a wide array of different stakeholders.

Governance frameworks will also have to be built around the current complex institutional ecology of internet governance, rather than seeking to control or replace it. Internet governance is currently dispersed and fragmented, with different institutions responsible for maintaining different elements of the system. For example, ICANN is responsible for assigning Internet Protocol addresses and domain names at the international level, whilst regional registries perform similar tasks at local levels. Standards and protocols that ensure that applications and equipment can communicate across the internet are developed in a range of organisations, including the ITU and W3C. The internet evolved to be what it is today because it was developed and maintained in this dispersed manner by communities of experts. Whilst we argue that it is necessary to develop a consistent and positive governance framework across a range of different policy spheres, this should be built around the current institutional ecology of internet governance institutions. However, there is a need to ensure that these institutions are more transparent and participatory, operating in the interests of the public rather than powerful stakeholder groups. The empowering aspects of the internet are rooted in the fact that it is a dispersed and fluid medium. Governance frameworks should seek to maintain these characteristics and be built from the bottom-up in a multi-stakeholder, accountable fashion. Attempts to exert governmental control from the top-down are likely not only to be ineffective, but also threaten to damage the aspects of the internet that we value it for.

Too often, communication policy is seen in instrumental terms – as an adjunct to development policy or as a tool to achieve another social goal such as improved health care or education. The media has always been an essential element of democracy and human rights, providing a platform for the public exercise of the human right to freedom of expression but also as a means of exchanging ideas, opinion and debate. Digital communications as they merge into the media sphere take on similar roles. It is therefore important to understand that the creation of communication capacity in itself is a social and public good. One of the lessons that can be learnt from the development of the digital world to date is that it is impossible to predict how technologies and applications will be invented and used. For example, a social networking application originally developed for US college students can become a major mobilising tool for public protest in repressive states. As it is impossible to predict the imaginative uses people make of technology, it is important to resource the creation of communication capacities rather than focusing on the development of tools or attempting to predict how they will be used. This may involve promoting education and literacy in key areas, encouraging the development of
open source hardware and software that provide a solid basis for innovation and adaptation according to need, and maintaining the openness of digital communications environments.

8.2 A window of opportunity for positive policy development

Digital communications are receiving increasing attention within a number of policy circles at national and international levels, providing a window of opportunity for the EU to make positive interventions in policy development. Firstly, the issues have been the subject of recent debate within the European Parliament itself, for example with the recent Recommendation on strengthening security and fundamental freedoms on the Internet. This document is principally concerned with balancing internet freedoms with measures necessary to combat terrorism, hate crime and cybercrime. While the recommendations are broadly progressive, applying this lens tends to emphasise human rights issues in which questions of balancing rights are of particular concern to policy makers. The focus is on balancing, rather than on developing positive policy frameworks for open communication. The document exhorts, in broad terms, participation in multi stakeholder processes to promote human rights standards and specifically standards for “data protection, security and freedom of speech”, without being specific as to what those standards might be or how they are to be defined. There is a need to build upon these important recommendations through further research and dialogue.

Secondly, a number of governments are starting to focus attention on digital communications and human rights within their bilateral and multilateral relations. A recent speech by US Secretary of State Hilary Clinton committed the US to “devoting the diplomatic, economic, and technological resources necessary to advance...internet freedom” (Clinton, 2010). Sweden adopted freedom of expression on the internet as a priority issue during its 2009 presidency of the European Union. Sweden has since committed itself to continuing to address these issues, with Carl Bildt, foreign secretary of Sweden, calling for “a new transatlantic partnership for protecting and promoting the freedoms of cyberspace.” He went on to say, “we must seek to shape the rules that will protect the rights and the freedom of cyberspace” (Bildt, 2010).

Thirdly, there are encouraging signs that human rights and ICTs are starting to receive more attention within the UN human rights system. UN human rights bodies have been notably absent from debates concerning internet governance and communications policy at the international level. However, the Special Rapporteur for the promotion and protection of the right to freedom of opinion and expression participated in the 2009 Internet Governance Forum. He is now working with the Swedish government to examine the implications of developments in internet technology and practice for freedom of expression, possibly with a view to submitting a report to the Human Rights Council.

Finally, a number of multi-stakeholder initiatives are making positive progress in defining and implementing standards to guide ICT policy and activity. For example, the Global Network Initiative has brought civil society, business and investors together to develop guidelines to help communications companies make informed and ethical decisions when they are requested by states to take actions that threaten human rights. In another example, Brazil has taken the lead in promoting inclusive and participatory internet governance through establishing a multi-stakeholder steering committee which is responsible for the coordination and integration of internet services in the country. The committee has recently adopted a set of principles to guide internet governance in Brazil which make a commitment to respecting freedom, privacy and human rights, democratic and collaborative governance, universality, diversity and innovation. At the international level, the mandate of the Internet Governance Forum is set to be renewed following almost unanimous agreement amongst business, government and civil society participants of the value of multi-stakeholder dialogue and cooperation.
These initiatives, and others like them, stem from a growing sense within a number of policy circles that there is a need to defend the democratic space created by digital communications against encroachment by those wishing to shut it down. This growing awareness provides the EU with a window of opportunity to engage in dialogue, taking the lead in fostering cooperation to build an enabling policy framework that expands the positive dimensions of digital communications and their capacity to support human rights.

8.3 Recommendations

The individual sections of this report have made recommendations of actions that the EU could take to address the impact that ICTs are having on freedom of expression, privacy, access to knowledge and culture, economic and social rights and equality. In short, there is a need for the EU to ensure that all of these human rights are upheld and advanced through both domestic and foreign policy. As discussed, this will require policy review, development and coordination across a range of different areas, from trade to development, intellectual property rights, media and data protection. Further research and analysis needs to be conducted to ensure that policy can effectively address new challenges, particularly in relation to balancing between human rights online and determining the liability and roles of different stakeholders and communication intermediaries.

The goal of these efforts should be to develop an international inclusive and participatory governance framework that promotes the empowering dimensions of digital communications. As well as developing consistent and constructive internal policy, the EU could focus on mobilising its diplomatic resources to this end. Options for doing this fall into four broad categories. The first is engagement in creative and coherent diplomacy and standard setting. Second, promoting awareness and understanding of the issues. Third, building foundations for stakeholder-led collaboration and problem solving. Fourth, developing expertise and providing direct support to human rights defenders. Each of these is addressed in turn below.

1) Creative and coherent diplomacy and standard setting

Bilateral dialogue: The EU conducts a number of human rights bilateral dialogues with countries such as China and, in the past, Iran. Questions of human rights and digital communication are becoming a feature of these dialogues and it is important that this continues.

Trade negotiations: When the Chinese government sought to introduce preloaded Green Dam Youth Escort software on all personal computers sold in China, U.S. trade officials called on China to readdress the policy, claiming that it could conflict with Beijing’s obligations under its membership of the World Trade Organisation. This is an example of how multi-lateral trade and business forums can be used to pursue agreements which would favour open technology and thereby advance human rights principles. The EU should be flexible in its thinking, examining the possibility of using such forums for diplomatic effect.

Working at the UN level: The EU should work to promote human rights-based communications policy in and through its cooperation with UN bodies, helping to mainstream consideration of human rights principles across the diverse issue areas that the UN covers, from development to intellectual property. There is an urgent need for guidance from the UN human rights bodies on balancing between human rights online and on the responsibilities and liability of different stakeholders and internet intermediaries. The EU could use the UN as a vehicle for making progress in these areas. Diplomatic pressure can also be applied through the United Nations, both directly through the UN Human Rights Council but also through special mechanisms such as the Special Rapporteur for Freedom of Opinion and Expression. One option could be to sponsor a resolution on digital communications and human rights.
2) Promoting awareness and understanding of the issues

Commissioning research: There are gaps in knowledge and evidence concerning a number of the issues raised in this paper. This leads to policy making being driven by popular perception and moral panic, for example in the arenas of cybercrime and child protection. In the arena of intellectual property protection, policy is based almost entirely on figures and arguments produced by the creative industries, and in particular multinational corporations. In order to formulate effective and pertinent policy, there is an urgent need for independent, in-depth research that examines the needs and opinions of citizens and users of digital communications and that takes public interest dimensions into account.

Facilitating dialogue and learning: There is scope for the EU to take the lead in organising events and bringing stakeholders together to advance understanding about the relationship between ICTs and human rights. During the Swedish presidency of the EU, a meeting was held in Warsaw with the Council of Europe and the OSCE’s Special Rapporteur for freedom of expression to examine how digital communications are impacting upon human rights. The EU could consolidate and build on the learning from this event, perhaps by hosting a larger scale event that could bring in other institutions and states, including the US government, the Canada, Australia and New Zealand bloc and potential allies on these issues from the global south, such as South Africa, India and Brazil. The EU could also host events and lead learning initiatives in existing fora, for example through holding workshops or best practice sessions on human rights and digital communications at the IGF.

Promoting communications and human rights literacy: Rather than focusing only on legislation and regulation, there is a need for people across the world to understand the opportunities and challenges presented by digital communications so that they can make informed decisions about how to behave and communicate online. Such approaches to improving communications literacy would help to preserve the fluid, innovative and creative dimensions of digital communications whilst at the same time empowering people to protect and expand their human rights.

3) Fostering multi-stakeholder collaboration and problem-solving

Promoting effective co-regulation: The dispersed and open nature of digital communications environments requires innovative approaches to regulation that are developed and maintained by direct stakeholders themselves. The EU could help to provide the incentives and structures that would enable such approaches to flourish. A growing number of communications companies are looking for alignments between their business interests and human rights values. To that end, the EU could launch talks with companies and other actors to identify areas of shared concern. These could include the export of technologies capable of being used to suppress dissent, as well more positive potential linkages between private investment opportunities and EU development aid. One promising initiative is the GNI. Whilst this is a partnership between civil society and business, the EU could play an important role in encouraging European companies and organisations to join the initiative.

Promoting innovation to advance human rights: The EU could help to explore the human rights potential of digital tools by establishing working partnerships with industry, academia, and nongovernmental organisations. This could involve establishing a forum to regularly review how digital communications technologies can be allied to wider EU human rights diplomatic goals. One obvious area of exploration is to look at the growth in the use of mobile phones and applications, and examine how these tools can help to empower people around the world and support traditional EU human rights diplomacy. A creative exchange forum could be established to bring together software developers, hardware companies and user groups to identify needs and opportunities. An innovation
fund could also be established (possibly to the value of Eur1m) to support innovation and sponsor the development of technologies or business ideas to support human rights in the digital world.

**Strengthening interaction and collaboration between stakeholders:** This report has stressed the importance of multi-stakeholder governance of digital communications. To be effective, this will require better relations between government, business and civil society actors than currently exist. The EU could help through actively participating in multi-stakeholder spaces and working groups. The EU has made good progress in this regard at the IGF, both through its support for the continuation of the Forum and through holding European consultations there that bring together member governments, parliamentarians and civil society. Further progress could be made through supporting and participating in the IGF dynamic coalitions – multi-stakeholder networks of people interested in collaborating on specific issues. The Internet Rights and Principles coalition is currently drafting a charter on Human Rights and Principles on the Internet, which is in line with the European Parliament’s 2009 recommendation to support an Internet Bill of Rights. There is also scope for the EU to push for increased transparency, inclusivity and public interest policy in internet governance institutions such as ICANN and the ITU. Participation of parliamentarians and commissioners in such initiatives would help to strengthen them, and promote multi-stakeholder working more generally.

4) **Providing expertise and direct support**

**Establishing an expert team within the External Action Service:** The new External Action Service (EAS) could use its resources to monitor possible abuses of human rights in the digital communications environment and use its diplomatic leverage to raise protests where necessary. The EAS could establish a digital communications and human rights team to back up the EU’s diplomatic efforts in this area. This would provide a source of expertise on the issues across the EU, as well as being a dedicated resource. The team could co-operate with its U.S. equivalent in the State Department – a proposed Civil Society 2.0 Initiative designed to help grassroots organisations enter the digital age.

**Building emergency action capabilities:** Natural disaster, conflict and humanitarian crises can severely disrupt and damage communication networks. The EU could establish a resource centre with equipment, training, mobile network deployment capacity and public education capacity designed to provide flexible and immediate information and media capacity to help alleviate human suffering in disaster or conflict situations.

**Supporting human rights defenders:** The EU could provide direct support to civil society networks and groups seeking to promote a human rights approach to digital communications through its aid mechanisms. There might be a specific focus on supporting the development of tools and policies that enable citizens to avoid politically motivated censorship, for example by providing funds to groups around the world with training and capacity building. This might be achieved by a specific Request for Proposals to invite networks or collaborations of NGOs to apply with their ideas on how best to achieve the objectives.

**Supporting ICT access within development cooperation:** The EU could support access to digital communications infrastructure in developing countries. Such projects could include providing investment or low cost loans for telecommunications infrastructure or community access projects. Support can also be provided in the development of meaningful and realistic ICT policies. The EU could also play a role in inserting consideration of digital communications into international aid policy and discourse. For example, ICTs could play a role in achieving mutual accountability between government and citizens that is required by the Paris Principles for Aid Effectiveness, and digital communications have a key role to play in helping to realise the Millennium Development Goals, both instrumentally and indirectly.
8.4 Concluding remarks

Taken together, these ideas represent a balanced range of responses to the complex challenge of developing digital communications environments that support and expand human rights. As illustrated throughout this report, this challenge cannot be met solely through government legislation and regulation. Digital communications have provided new opportunities for human rights because of the new capacities that technological developments have made possible; because of innovation by businesses aiming to provide what users want; and most importantly by the human ingenuity of users harnessing new technological opportunities to meet their needs and wants. The EU has an important role to play on the world stage in expanding these opportunities for innovation and further positive development of communications technology. This will require coordinated action to promote positive policy frameworks that are rooted in, and that promote, human rights and public interest principles at national and international levels.
REFERENCES


AFP (2010) Opposition attacks Belarus Internet crackdown February 2, 2010 http://www.google.com/hostednews/afp/article/ALeqM5q0AWZ61GmS71kYLpCloW7m1akvbw (Last accessed 14/05/10)


Alampay, E. and Bala, G. (2009) Mobile 2.0: m money for the BOP in the Philippines Lirne Asia Mobile 2.0 Project paper.


BBC News (2010a) Mobile that allows bosses to snoop on staff developed March 10, 2010 http://news.bbc.co.uk/1/hi/technology/8559683.stm (Last accessed 16/04/10)

BBC News (2010c) Internet access is a “fundamental right” March 8, 2010 http://news.bbc.co.uk/1/hi/8548190.stm (Last accessed 16/04/10).


Atlantic Magazine http://www.theatlantic.com/magazine/archive/2008/07/is-google-making-us-stupid/6868/ (Last accessed 16/04/10)


Committee on Economic, Social and Cultural Rights (2005) *General Comment 17: The right of everyone to benefit from the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he or she is the author (article 15, paragraph 1 (c), of the Covenant)* Thirty fifth session, Geneva, 7 25 November 2005


http://www.chathamhouse.org.uk/research/security/papers/view/-/id/702/ (Last accessed 16/04/10)

Council of Europe (1950) *Convention for the Protection of Human Rights and Fundamental Freedoms*

http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm (Last accessed 16/04/10)

http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (Last accessed 16/04/10)


Council of Europe (2008) *Recommendation CM/Rec(2008)6 of the Committee of Ministers to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters* March 26, 2008

http://www.coe.int/t/informationsociety/documents/HR%20guidelines%20for%20Internet%20service%20providers_en.pdf (Last accessed 16/04/10)

http://www.coe.int/t/informationsociety/documents/HR%20guidelines%20for%20online%20games%20providers_en.pdf (Last accessed 16/04/10)


Council of the EU (2010a) *HR’s declaration on behalf of the EU on the situation in Belarus* Brussels March 31, 2010

Council of the EU (2010b) *Council Resolution of 1 March 2010 on the enforcement of intellectual property rights in the internal market.* 2999th COMPETITIVENESS Council meeting

http://www.indexoncensorship.org/2010/03/cyber-wars-technology-deiber/ (Last accessed 16/04/10)


http://googleblog.blogspot.com/2010/01/new-approach-to-china.html (Last accessed 14/05/10)

http://googleblog.blogspot.com/2010/03/new-approach-to-china-update.html (Last accessed 14/05/10)


EC Information Society [a], *The Telecoms Reform*  

EC Information Society [b], *Main elements of the reform*,  


http://www2.ohchr.org/english/issues/terrorism/rapporteur/docs/A_HRC_13_37_AEV.pdf (Last accessed 16/04/10)

http://a330.g.akamai.net/7/330/25828/20081210173751/graphics.eiu.com/upload/Intel_Digital_Divide.pdf (Last accessed 14/05/10)

http://www.edri.org/edrigram/number12/parody-website-germany (Last accessed 16/04/10)

http://www.edri.org/edrigram/number5.12/cybercrime-convention-dangerous (Last accessed 16/04/10)

http://www.edri.org/edrigram/number8.6/ipr-enforcement-report-ep (Last accessed 16/04/10)

EDRI (2010a) *EDRi sends open letter to EU Commissioners to oppose Internet blocking* 10 March 2010  
http://www.edri.org/edrigram/number8.5/edri-open-letter-internet-blocking (Last accessed 06/05/10).  

EPIC[a] *Privacy and Consumer Profiling* http://epic.org/privacy/profiling/ (Last accessed 16/04/10)  

EPIC[b] WHOIS http://epic.org/privacy/whois/ (Last accessed 16/04/10)  

EPIC[c] Social Networking Privacy http://epic.org/privacy/socialnet/ (Last accessed 16/04/10)  

EPIC[d] Facebook Privacy http://epic.org/privacy/facebook/ (Last accessed 16/04/10)  

EPIC[e] Cloud Computing http://epic.org/privacy/cloudcomputing/ (Last accessed 16/04/10)  

EPIC[f] Search Engine Privacy http://epic.org/privacy/search_engine/ (Last accessed 16/04/10)  

92


Geist, M. (2010) *ACTA Draft Text Released: (Nearly) Same As It Ever Was* April 21, 2010 [http://www.michaelgeist.ca/content/view/4972/125/](http://www.michaelgeist.ca/content/view/4972/125/) (Last accessed 12/05/10)


Human Rights Council (2009) *Promotion and Protection of all Human Rights, Civil, Political,*


http://www.nature.com/nature/journal/v449/n7158/full/449038a.html (Last accessed 16/04/10)


http://www.boston.com/bostonglobe/ideas/articles/2009/09/20/project_gaydar_an_mit_experiment_r aises_new_questions_about_online_privacy/ (Last accessed 16/04/10)

http://cecc.gov/pages/hearings/2010/20100324/jonesTestimony.pdf?PHPSESSID=0a21d5e48e9109f8263da02ae7b37d61 (Last accessed 16/04/10)


http://blogs.ssrc.org/datadrip/?p=176#more-176 (last accessed 16/04/10)


Kee, J.S. (2005) Probing the Texture of Silence in Communications and Media at B + 10

Kee, J.S. (2010) Beyond tools: Internet as a critical policy issue for the advancement of women's rights


http://www.osce.org/publications/dfm/2004/12/12239_89_en.pdf (Last accessed 14/05/10)


http://www.lse.ac.uk/collections/EUKidsOnline/Reports/Default.htm (Last accessed 16/04/10).


http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2378/2089 (Last accessed 16/04/10)

MacKinnon, R. (2010) Google and Internet Control in China testimony submitted for the record by
MacKinnon for the Congressional-Executive Commission on China, March 24, 2010


(Last accessed 16/04/10)

and Terrorism 27(4) pp 297 – 319

http://googleblog.blogspot.com/2006/01/google-in-china.html (Last accessed 14/05/10)

McNamee, J. (2010) Pointless action on child pornography Guardian Comment Is Free article, March 29
(Last accessed 06/05/10)

Muente-Kunigami and Navas-Sabater (2009), Options to Increase Access to Telecommunications Services in Rural and Low-Income Areas, The World Bank


OECD (1980) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html (Last accessed 16/04/10)


ONI (2009a) Internet Filtering in Egypt http://opennet.net/sites/opennet.net/files/ONI_Egypt_2009.pdf (Last accessed 16/04/10)

ONI (2009c) China http://opennet.net/research/profiles/china (Last accessed 16/04/10)

ONI[a] About Filtering http://opennet.net/about-filtering (Last accessed 16/04/10)


 Reuters (2009a) *Internet most popular information source; poll* June 17, 2009 http://www.reuters.com/article/idUSTRE55G4XA20090617 (Last accessed 16/04/10)


Schulman, A. (2001) The Extent of Systematic Monitoring of Employee E-mail and Internet Use Privacy Foundation July 9, 2001 http://www.sonic.net/~undoc/extent.htm (Last accessed 16/04/10)


Souter, D. (2009c) Information and Communications Development Applications in APC ICT Policy Handbook The Association for Progressive Communications, ed. Souter D.
http://www.delvie.ec.europa.eu/enieu_osce/eu_statements/2010/February/PC%20no.794%20-%20EU%20on%20media%20situation%20in%20BELR.pdf (Last accessed 14/05/10)


Telegraph (2009a) China has not given up Green Dam plan July 2, 2009 http://www.telegraph.co.uk/news/worldnews/asia/china/5720396/China-has-not-given-up-Green-Dam-plan.html (Last accessed 16/04/10)


The Times (2009) India to issue all 1.2 billion citizens with biometric ID cards July 15, 2009 http://www.timesonline.co.uk/tol/news/world/asia/article6710764.ece (Last accessed 16/04/10)


http://www2.ohchr.org/english/law/cescr.htm (Last accessed 16/04/10)

UN (1979) *Convention on the Elimination of All Forms of Discrimination against Women* December 18, 1979,
http://www.un.org/womenwatch/daw/cedaw/text/econv.htm (Last accessed 16/04/10)


http://www2.ohchr.org/english/law/crc.htm (Last accessed 16/04/10)

http://www2.ohchr.org/english/law/disabilities-convention.htm (Last accessed 16/04/10)


W3C working draft: *How People with Disabilities Use the Web*

http://online.wsj.com/article/SB124562668777335653.html (Last accessed 14/05/10)

WGIG (2005) *Working Group on Internet Governance Report*
http://www.wgig.org/docs/WGIGREPORT.doc (Last accessed 16/04/10)


WIPO (2007) *The 45 Adopted Recommendations under the WIPO Development Agenda*

WIPO[a] *How do technological protection measures work?*
http://www.wipo.int/enforcement/en/faq/technical/faq03.html (Last accessed 16/04/10)

http://news.yahoo.com/s/ap/20100325/ap_on_hi_te/as_tec_china_google_search_comparison (Last accessed 14/05/10)
http://www.itu.int/wsis/docs/geneva/official/dop.html (Last accessed 16/04/10)

http://www.itu.int/wsis/docs/geneva/official/poa.html (Last accessed 16/04/10)


WSIS[a] *Basic Information: About WSIS*. WSIS Website http://www.itu.int/wsis/basic/about.html (Last accessed 16/04/10)


POLICY DEPARTMENT

Role
Policy departments are research units that provide specialised advice to committees, inter-parliamentary delegations and other parliamentary bodies.

Policy Areas
Foreign Affairs
   Human Rights
   Security and Defence
Development
International Trade

Documents