Freedom of Connection – Freedom of Expression:
The Changing Legal and Regulatory Ecology Shaping the Internet

by

William H. Dutton
Anna Dopatka
Michael Hills
Ginette Law
and
Victoria Nash

Oxford Internet Institute
University of Oxford
1 St Giles Oxford OX1 3JS
United Kingdom

29 November 2010

A report prepared for UNESCO's Division for Freedom of Expression, Democracy and Peace. The opinions expressed in this report are those of the authors and do not necessarily reflect the views of UNESCO or its Division for Freedom of Expression, Democracy and Peace.

Preface

As stated in its Constitution, UNESCO is dedicated to 'Promot(ing) the free flow of ideas by word and image'. Part of this mission, therefore, is to promote freedom of expression and freedom of the press through sensitization and monitoring activities, as a central element in building strong democracies, contributing to good governance, promoting civic participation and the rule of law, and encouraging human development and security. Media independence and pluralism are fostered by the Organization, providing advisory services on media legislation and sensitizing governments and parliamentarians, as well as civil society and relevant professional associations. However, UNESCO recognizes that the principle of freedom of expression must apply not only to traditional media, but also to the Internet. Providing an unprecedented volume of resources for information and knowledge, the Internet opens up new opportunities for expression and participation and holds enormous potential for development.

This comprehensive research publication examines the changing legal and regulatory ecology that has shaped the Internet over the years. The research was supported by UNESCO within the framework of the follow-up process to the World Summit on the Information Society, and as part of UNESCO's activities relating to the Internet Governance Forum. The principle aim was to provide a reference tool that can inform and stimulate the current debate on the global trends that have shaped freedom of expression on the Internet. The report explores the various legal and policy mechanisms that are crucial for the free flow of information, providing guidance for policy-makers and other relevant users on the creation of environments conducive to the freedom of expression.

As this publication makes clear, freedom of expression is not just a by-product of technical change; it must be protected by legal and regulatory measures that balance a variety of potentially conflicting values and interests in a complex global ecology of choices. The impetus that this report provides for the prioritization of research in this field encourages further scrutiny of the multifaceted issues that govern the conditions for freedom of expression on the Internet. The findings of this research point to the need to better track a wider array of global legal and regulatory trends, and whether individual researchers, students or policy makers, it is my hope that this publication proves to be a useful and informative resource for all readers.

Jānis Kārkliņš, Assistant Director-General for Communication and Information, UNESCO

Acknowledgements

Support of this report was provided by UNESCO's Division for Freedom of Expression, Democracy and Peace and by the Fifth Estate Project at the Oxford Internet Institute (OII), through gifts from June Klein, Electronic-Boardroom TMV®. Many others helped in the preparation of this manuscript. We are particularly grateful to a group of advisors we assembled to alert us to key legal and regulatory trends, and review interim drafts of our report. Our advisory committee included:

Ian Brown, a computer scientist and Senior Research Fellow at the OII, with expertise in computer security and privacy.

David Erdos, a legal scholar at Balliol, College, Oxford and the Katzenbach Research Fellow at the Centre for Socio-Legal Studies, Faculty of Law, Oxford.

Christopher Millard, OII Senior Fellow and Professor of Privacy and Information Law, School of Law, Queen Mary, University of London.

Richard Susskind, OII's Visiting Professor in Internet Studies, with expertise in the role of Information Technology and the Internet in legal professions.

Tracy Westen, Director, Center for Government Studies in Los Angeles, and Adjunct Professor, at the University of Southern California's Annenberg School.

Jonathan Zittrain, Professor at the Berkman Center at Harvard University, and a founding director of the OpenNet Initiative.

In addition, we are very grateful to Bianca Reisdorf for assistance with the preparation of tables and figures, Mahmood Enayat for observations on Iran, Louise Guthrie and Arthur Thomas for comments on ratings, Alissa Cooper for her perspective on network neutrality, and Arthur Bullard for his help with figures. We owe special thanks to staff of UNESCO's Division of Freedom of Expression, Democracy and Peace, especially Mogens Schmidt and Xianhong Hu, for comments and guidance.

An earlier version of this report was presented for a workshop at the 2010 Internet Governance Forum in Vilnius. We thank UNESCO for organizing this workshop and those attending who offered constructive comments that have helped us to improve this manuscript.

William Dutton
Anna Dopatka
Michael Hills
Ginette Law
and
Victoria Nash

Executive Summary

Over the first decade of the 21st Century, the Internet and its convergence with mobile communications has enabled greater access to information and communication resources. In 2010, nearly 2 billion people worldwide – over one quarter of the world's population – use the Internet. However, during the same period, defenders of digital rights have raised growing concerns over how legal and regulatory trends might be constraining online freedom of expression. Anecdotal accounts of the arrests of bloggers, the filtering of content and the disconnection of users have sparked these concerns. However, they are reinforced by more systematic studies that provide empirical evidence of encroachments on freedom of expression, such as through the increased use of content filtering.

This report provides a new perspective on the social and political dynamics behind these threats to expression. It develops a conceptual framework on the 'ecology of freedom of expression' for discussing the broad context of policy and practice that should be taken into consideration in discussions of this issue. This framework draws on an original synthesis of empirical research and case studies of selected technical, legal and regulatory trends. These include developments in six interrelated arenas that focus on:

1. technical initiatives, related to connection and disconnection, such as content filtering;
2. digital rights, including those tied directly to freedom of expression and censorship, but also indirectly, through freedom of information, and privacy and data protection;
3. industrial policy and regulation, including copyright and intellectual property, industrial strategies, and ICTs for development;
4. users, such as measures focused on fraud, child protection, decency, libel and control of hate speech;
5. network policy and practices, including standards, such as around identity, and regulation of Internet Service Providers; and
6. security, ranging from controlling spam and viruses to protecting national security.

By placing developments in these arenas into a broad ecology of choices, it is more apparent how freedom can be eroded unintentionally as various actors strategically pursue their own diverse array of objectives. The findings reinforce the significance of concerns over freedom of expression and connection, while acknowledging countervailing trends and the open future of technology, policy and practice. Freedom of expression is not an inevitable outcome of technological innovation. It can be diminished or reinforced by the design of technologies, policies and practices – sometimes far removed from freedom of expression. This synthesis points out the need to focus systematic research on this wider ecology shaping the future of expression in the digital age.

Table of Contents

Introduction

Legal and Regulatory Trends Shaping Freedom of Expression

The continuing reinvention and worldwide diffusion of the Internet has made it an increasingly central medium of expression of the 21st century, challenging the role of more traditional mass media, including radio, television, and newspapers. In 2010, nearly 2 billion people worldwide – over one quarter of the world's population – use the Internet.[1] This could have major societal implications, as the use of the Internet has the potential to reshape global access to information, communication, services, and technologies (Dutton 1999, 2004). Enduring issues, ranging from freedom of the press to the balance of world information flows in all sectors, and from the media to the sciences, will be tied to the Internet as a 'network of networks' – an interface between individuals and the news, information, stories, research, cultures and entertainment flowing worldwide (Baer et al 2009).

The increasing centrality of the Internet has countervailing implications. On the one hand, the global diffusion of the Internet, along with a continuing stream of innovations, such as the ease with which users can create as well as consume text and video, are making the Internet increasingly pivotal to the communicative power of individuals, groups and institutions with access to networks and the skills to use them effectively (Dutton 2005; Castells 2009).

On the other hand, this very shift in communicative power has spawned greater efforts to restrict and control the use of the Internet for information and communication on political, moral, cultural, security, and other grounds. It is leading also to legal and regulatory initiatives to mitigate risks associated with this new medium, ranging from risks to children, to privacy, to intellectual property rights, to national security, which might more indirectly, and often unintentionally, enhance or curtail freedom of expression. In some cases, limits on expression are intentional, but often unintended, such as when regulatory instruments, that might have been appropriate for newspapers, broadcasting or the press, are used inappropriately to control the Internet.[2]

As a consequence, defenders of freedom of expression have raised growing concerns over how legal and regulatory trends might be constraining freedom of expression at the very time that the Internet has become more widely recognized as a major medium for fostering global communication. These concerns are reinforced by surveys that provide evidence of encroachments on freedom of expression, such as through the filtering of Internet content. At the same time, despite Internet censorship and filtering, this network of networks continues to bring more information to increasing numbers of individuals around the world, particularly as mobile communication extends its reach to vast numbers of individuals without access to more traditional communication resources. However, technological innovation will not necessarily enhance freedom of expression. It is not a technologically determined outcome or an inherent consequence of Internet use. This report argues that it will be diminished unless freedom of expression is explicitly and systematically addressed by policy and practice.

This report provides a preliminary view of the evidence behind these concerns, and how they can be addressed through more systematic research, and new frameworks for discussion of policy and practice. It is not a definitive treatment of the wide-ranging issues it addresses, but an effort to begin an original overview and synthesis of legal and regulatory trends that could reshape freedom of expression in the digital age of networked societies.[3] In doing so, it offers a framework that places developments within a broad ecology of actors, objectives, and strategies for shaping the role of the Internet and Web in local and global communication, based on a critical review of existing research, legal and regulatory documentation, news coverage, and expert opinion. The findings reinforce the significance of these concerns, while acknowledging countervailing trends and the uncertain future of freedom of expression. Based on these findings, the report points toward a need to more systematically monitor a wide range of legal and regulatory developments that directly–and indirectly– shape the future of free expression on the Internet in local and global contexts.

This synthesis also suggests a need for further research to systematically monitor these developments in ways that are trusted and able to inform debate about policy and practice. Ultimately, the Internet's great potential contribution to political and democratic institutions and processes will depend on such monitoring and oversight.

Freedom of Expression in a Network Society

Representatives of global institutions and national governments around the world have endorsed freedom of expression as a basic human right. While most often associated with freedom of the press and the First Amendment in the US, freedom of expression is not only an American value. It has been upheld as a basic human right for decades by a number of international organizations, having been endorsed since 1948 in the United Nations Universal Declaration of Human Rights.[4]

In 2009, speaking to college students in Shanghai, China, on his first Asian trip as President of the United States, Barack Obama, made this point. He cited freedom of expression, along with religion, as a universal human right, saying:

> '… freedoms of expression, and worship, of access to information and political participation – we believe they are universal rights. They should be available to all people, including ethnic and religious minorities, whether they are in the United States, China or any nation.'[5]

This position was reinforced and extended by US Secretary of State, Hillary Rodham Clinton (2010), in linking freedom of expression in the 21st Century with the right of people to connect. She evoked the First Amendment to the US Constitution, and Franklin Roosevelt's 'Four Freedoms' speech of 1941, to discuss freedom of expression on the Internet and extend this to what she called the freedom to connect, defined as the 'idea that governments should

not prevent people from connecting to the [I]nternet, to websites, or to each other'. She also spoke of a need for 'freedom of assembly in cyber space'.

In many states, the right to free expression is augmented by rights to freedom of information, providing citizens with a legal right to request and access government-held information, and imposing duties on states to publish open records. The close connection between these rights is obvious, namely that the value of free expression is significantly weakened if it cannot be exercised in consideration of key political information relating to how citizens are governed and taxes spent. The importance of this connection was expressed by Viviane Reding (2007), Commissioner for Information Society and Media in the European Commission, in saying: 'Freedom of expression is one of the most fundamental rights of our European democracies' ... but that 'without freedom of information, freedom of expression often remains meaningless'. These recent developments reinforce the commitment of international institutions, such as UNESCO, which 'promotes freedom of expression and freedom of the press as a basic human right'.[6]

The logic underlying the defence of these values is two fold. One is that the free flow of ideas is critical to democratic processes and institutions, such as the ability of citizens to vote in an informed way and to hold their governments and other public institutions accountable. A second is based on the priority placed on the autonomy of the individual in relation to larger collectives, a principle that varies cross-culturally, underpinning many debates over the relative weight given to individuals versus communities or other collectivities. For example, a focus on individual autonomy might support the role of the individual in choosing what to filter. In contrast, a focus on the collective could support a greater role for state filtering to protect shared values.

Clearly, freedom of expression is not absolute in any cultural setting and this applies equally, whether considering expression online or offline. Box 0.1 introduces Freedom House's typology of limits to freedom online. Cross-nationally and cross-culturally, the relative priority accorded freedom of expression in relation to many other goals and objectives, such as national security or personal privacy, is one of the critical issues tied to global governance of the Internet and related information and communication technologies (ICTs).

Box 0.1. Three Aspects of Freedom Online.[a]

Freedom House identifies three possible ways in which freedom on the Internet can be limited. These can be mapped onto our two categories, although all overlap and are interrelated:

1. Obstacles to access, including restrictions imposed by governmental policy or economic conditions, such as a lack of infrastructure;
2. Limits to content, such as through self- or government-censorship, when self-censorship includes that imposed by the Internet industry;
3. Restrictions on the rights of users, such as (un)lawful disconnection.

[a] Adapted from Freedom House (2009).

21st century conceptions of freedom of expression entail at least two general categories of rights tied to the Information Age of networked communication (Klang and Murray 2005: 1). The first focuses on access to the means for expression. In the age of digital networking, this increasingly translates into access to the Internet – one critical aspect of connection, and related ICTs, as they are becoming a primary interface between individuals and the world (Dutton 1999; Baer et al 2009). For this reason, the global diffusion of the Internet has become a critical issue for those supporting worldwide freedom of expression.[7]

The second focuses on the rights of individuals and groups to use various media, from association to mass communication in order to support political processes and institutions, such as elections, but also in all areas of life. This is most often associated with freedom of the press and the freedom to associate with others, but increasingly freedom of expression is being extended to the requirement of rights to use the Internet and ICTs for obtaining information and organizing politically, particularly as individual Internet users increasingly take on many roles formerly played by the press.

The Internet as a worldwide 'network of networks' could enable people to inform and educate themselves, express their views, and participate in civil society and democratic processes to an extent never before possible. New forms of information and participation like Internet-based newspapers, blogs, or social networking sites are challenging more traditional media by proposing new forms of communication, such as by enabling users to share, generate and even co-create or co-produce information (Table 1). In such ways, the Internet has complemented more traditional forms of one-to-many broadcast communication by many-to-many and many-to-one networks of communication, as illustrated by the work of Global Voices (Box 0.2). Such initiatives over the Internet are expected to enhance the diversity of available information and facilitate access to 'user-generated content' (UGC) in ways that empower citizens, and become a tool for ensuring greater transparency and openness.

Table 1. Forms of Communication Enabled by the Web[a]

Web-enabled	**Illustrations**
Web 1.0. Sharing Information	Hypertextual links on the Web, enabling the global sharing of documents, text, video, etc.
Web 2.0. User-generated content (UGC)	Blogging, micro-blogging (e.g., Twitter), User comments, ratings, polling, etc.
Web 3.0. Co-creation, co-production of information	Wiki-based contributions (e.g., Wikipedia), collaboration software (e.g., Google Docs)

[a]Adapted from Dutton (2009).

Box 0.2. Global Voices: Complementing and Extending Traditional Media.

Global Voices is a collaboration, claiming more than 200 bloggers around the world, that works on translations and reports from blogs and citizen media outlets. They place an emphasis on giving voice to people and views that are not ordinarily heard on international mainstream media and therefore not likely to reach a broad audience. The Global Voices team also has an Advocacy website and network designed to help people express opinions online in countries where their voices are restricted by state censorship.

See: http://globalvoicesonline.org

However, this potential for the Internet to enhance freedom of expression is not universally welcomed. For example, some worry that the Internet could undermine traditional media practices and institutions by eroding standards of broadcasting, undermining local and national media outlets and productions, or undermining the business models supporting the media, such as advertising or the sale or sharing of copyrighted material. In other cases there are concerns about particular information or content that might be disseminated online, perhaps on the basis of national security, or on political or moral grounds, such as in the case of WikiLeaks (see Box 0.3) distributing documents on the war in Afghanistan, which might have jeopardized the lives of informants identified in leaked documents (Waters 2010).

Box 0.3. WikiLeaks and the Wars in Afghanistan and Iraq

The Website WikiLeaks is dedicated to providing access to information by protecting 'whistleblowers, journalists and activists who have sensitive material to communicate to the public'.[a] The site leads with a quote from *Times Magazine* that the site '… could become as important a journalistic tool as the Freedom of Information Act.' It was founded and led by Julian Assange, based in Reykjavik, Iceland, on the notion that 'principled leaking' of key documents can support greater public accountability, invoking the spirit of Daniel Ellsberg and the Pentagon Papers. The site was supported primarily by individual volunteers, but the release of notable documents led to some funding through donations (Khatchadourian 2010).

On 25 July 2010, the site became a focus of debate over its posting of an 'Afghan War Diary, 2004-2010' on 25 July, which included over 91,000 reports on a dedicated Web page. WikiLeaks removed about 15,000 reports from the total archive as part of a 'harm minimization process demanded by our source'[b], but this did not prevent the release of information deemed sensitive by governments, the press, and civil liberties advocates, such as the identities of some informants. There were previous attempts to censor the site, such as in Australia, where the government included WikiLeaks pages in its censorship list (Singel 2009). This was followed in October 2010 by the release of documents related to the war in Iraq[c], reigniting controversy over the propriety and risks of confidential files being released.

[a] From 'about page' of WikiLeaks: http://wikileaks.org/wiki/WikiLeaks:About
[b] http://wikileaks.org/wiki/Afghan_War_Diary,_2004-2010
[c] http://wikileaks.org/

The use of Internet filtering (Box 0.4) and other means of restricting full access to the Internet has led to a number of efforts to track and monitor its prevalence, such as work done by Freedom House (2009), as well as academic research including the OpenNet Initiative. (Box 0.5).

Box 0.4. Internet Filtering

Governments, Internet Service Providers (ISPs), Internet access providers, companies, parents, or individuals can install software that restricts content to users. This software can be installed on an individual personal computer, but may also be installed 'upstream' on a home, company or ISP network server. In some cases, it is installed at a national 'backbone' level. A filter can screen particular words, email addresses, Web sites or other addresses and be used for example, if the installer wishes to prevent users within its borders from seeing particular content or a particular site. This software is sometimes called 'content-control' or 'Internet filtering' software. When used by governments, it is often branded as 'censorship', particularly if aimed at political speech. But in the case of ISPs, where filters are used for example to combat SPAM, it can be viewed as an essential service to users. In the household, parents might use a filter as a means of 'child protection'. These examples underscore the need to assess the social and political context in which filtering is conducted.

Box 0.5. The OpenNet Initiative

The OpenNet Initiative seeks to discover and report on the Internet filtering practices of countries that may be filtering Internet content for social (moral), political or security purposes. Their research team has employed creative mechanisms to obtain empirical evidence about what content is filtered in different countries, such as by making similar requests for Web pages from computers located within different nations. In addition to the study of Internet filtering, the project seeks to understand their outcomes and unintended consequences. The team does comparative assessments across countries, and writes regional overviews as well as country profiles on censorship and filtering to inform public policy makers and civil society advocates. OpenNet is a collaborative partnership of academic institutions, which includes the Citizen Lab at the Munk Centre for International Studies, University of Toronto; the Berkman Center for Internet & Society at Harvard University; and the Advanced Network Research Group at the Cambridge Security Programme, University of Cambridge.

See: Deibert et al (2008, 2010) and http://opennet.net/

Many different actors can restrict freedom of expression online. Individuals decide what to read, and what to delete or filter, such as by installing spam filters on their personal computer. Parents, corporate IT departments, and many other actors have a role in deciding what content is available to users in different social contexts. In general, however, studies of censorship and filtering and freedom of expression, generally, are most often concerned with governmental censorship. Governments can directly, or indirectly (through formal and informal agreements with ISPs), restrict freedom of expression by regulating access to the Internet or to particular Internet content. Many civil society advocates of freedom of expression are concerned that state-

supported restrictions on Internet access and information are increasing and thereby threatening freedom of expression online.

Whilst state-led filtering or censorship may be the most obvious and most feared threat to freedom of expression online, the most numerous challenges stem from the daily decisions of multiple different actors pursuing a diverse range of policy goals, many seemingly unrelated to freedom of speech at all. It is in the pursuit of these diverse objectives that their actions can (with or without intent) expand or limit citizens' enjoyment of freedom of expression. In some cases, the pursuit of particular goals can enhance freedom of expression. For example, the push towards economic progress by developing countries has been a major impetus behind the worldwide diffusion of the Internet, as it has become a central infrastructure for local and global economic transactions and trade. In other cases, the pursuit of different goals can lead, directly or indirectly, to restrictions of freedom of expression, such as where intellectual property legislation limits the free exchange of scientific research. These examples raise complicated and unresolved questions about legal and regulatory trends in related areas that might have more or less direct implications on freedom of expression on the Internet. This complex and evolving ecology of law and policy is the focus of this report.

It should be noted from the outset that this report does not seek to evaluate the relative significance of the different legal and regulatory trends for freedom of expression online. Clearly, some limitations on expression are more serious than others: persistent and concerted efforts by a government to block critical political comment is clearly a greater threat to personal freedom than the blocking of a website devoted to racist hate speech. Yet many of the regulatory and legal measures described in this report cannot be so clearly evaluated and weighed up, especially when the plural values of diverse modern states are taken into account. As such the main contribution of this report is to draw attention to the wide range of factors which may limit freedom of expression online, and judgments of significance or potential risk are left to the individual reader.

Outline of this Report

This report provides a synthesis of many of the key trends in law and regulation that might be reshaping freedom of expression around the world. It begins by providing a brief overview of previous literature and research on freedom of expression, which identifies key limitations of work in this area. The review leads us to introduce a framework for considering the many areas of policy and practice that need to be considered, which we call an evolving 'ecology of freedom of expression'. This framework provides a structure for discussing a broader array of policy choices than are not normally considered in discussions of freedom of expression, and establishes the significance of several key policy areas that are described in the following sections of the report, ranging from access to the Internet to concerns over national security.

Section 1 of the report undertakes a critical analysis of the literature on freedom of expression, arguing that it has not been sufficiently examined from a broad social science perspective, partly due to the politically sensitive features of this topic. Section 2 then establishes the 'ecology of freedom of expression' framework. The report then moves, in Section 3 into a discussion of the key elements of this ecology, beginning with an overview of one of the most positive developments, the worldwide diffusion of access to the Internet. This discussion looks at some of the legal and regulatory underpinnings of the widespread diffusion of the Internet that enables its potential as a means for empowering individuals and groups across the world.

Section 4 provides an overview of countervailing technical developments designed to filter the Internet. Here we argue that new technology is enabling the exercise of worldwide freedom of expression, but also providing governments with new forms of censorship and new ways to disconnect people from information and communication resources.

Building on this claim, Section 5 provides a meta-analysis of evidence regarding worldwide practice. This shows that a sizeable group of nations, including many that are commonly viewed as liberal democracies, are limiting freedom of expression for a variety of reasons, ranging from national security to moral concerns.

This analysis is followed by a discussion of five broad policy areas that are shaping freedom of expression online. Section 6 covers legal and regulatory efforts to protect other rights, such as community standards of decency, equality, freedom of information, privacy and data protection. This is followed in Section 7 by discussion of moves to stimulate and protect economic development and industrial goals, including the protection of intellectual property, and technology-led industrial and development strategies. Section 8 addresses the regulation of users, mainly by laws that apply offline and online to protect children and other individuals from harm, whilst Section 9 describes developments in Internet governance and regulation, focusing on competing models for regulating the Internet. Finally, in Section 10 we look at the area of security, a prime motivation behind some governments' efforts to filter.

The report concludes with a discussion of the value of the ecology of freedom of expression as a framework for study and policy deliberation, and of the need for further research to refine and extend this preliminary analysis, and ends with a set of recommendations for research, policy and practice.

1. Internet Freedom: A Perspective on the Research

The Literature

This report provides a synthesis of existing research and literature on freedom of expression in the digital age. It is not based on new data gathering, but aims at pulling data and research together in new ways and identifying areas for further research. We therefore provide only a brief overview of the existing literature, which is then woven throughout this report. However, it is important to present a broad sense of the literature in this field and indicate why it led us to propose a reconsideration and expansion of empirical research in this area, and also underline why we recommend the re-focusing of research on the larger ecology of freedom of expression on the Internet.

The literature in this field includes outstanding work that is theoretically and empirically innovative and significant. For example, the 1980 report of the McBride Commission (Box 1.1) has had a major impact on debate over global communication and remains relevant to discussions of the Internet and mobile communications. As the Internet promises to reconfigure global information flows, it will be important to revisit many aspects of the McBride Commission in the coming years.

Box 1.1. The MacBride Commission and Report

Sean MacBride, a Noble Peace Prize laureate from Ireland, presided over the International Commission for the Study of Communication Problems. This commission was established in 1977 by UNESCO, and reported in 1980 with the publication of *Many Voices One World* (ICCP 1980), which came to be known as the MacBride Report. This report became a major reference for advocacy of a 'New World Information and Communication Order' (NWICO). The Commission raised concern over the uneven international flow of news and information worldwide, which was protected by the advocacy of a free press. In calling for a new world information order, the report challenged conventional wisdom concerning the free flow of information in order to reduce or eliminate 'situations of political, economic and cultural dominance and dependence' on producers in the most developed nations (Ibid, p. 43). Despite an expressed commitment by the Commission to the principle of freedom of expression, the NWICO came to be viewed as an argument against the operation of the free market in global communication, and a threat to a press free of governmental oversight and control.

More contemporary research, such as that focused on Internet filtering, particularly that by the OpenNet Initiative, has developed creative approaches to gathering empirical data on the extent and nature of content filtering in a growing number of nations (Box 0.5, above). In addition, a number of Non Governmental Organizations (NGOs), for instance, Freedom House (FH) and Reporters without Borders, have invested heavily in monitoring governmental efforts to restrict freedom of expression (Freedom House 2009; Reporters

without Borders 2010). Studies such as these provide an empirical basis for informing debate and further research.

Limitations of Advocacy and Research

However, these studies and reports remain exceptional cases in a literature that has important limitations taken as a whole. Generally, with notable exceptions such as those identified above, the significance of the issues tied to freedom of expression has not been well matched by systematic programmes of independent, disinterested, research. In contrast, it has been generally:

- under-researched in light of early and continuing risks to freedom of expression;
- composed primarily of normative policy advocacy rather than empirically-anchored description and synthesis;
- focused most often on single issues, such as freedom of expression, child protection, or copyright, rather than on the tradeoffs among these often conflicting values and interests;
- limited to single indicators of trends in selected countries, such as the prominence of filtering in the countries most actively involved, rather than multiple indicators across systematic samples of countries;
- North American and European-centric in perspective, with freedom of expression being viewed as a particularly American priority, given the press freedoms tied to the First Amendment to the US Constitution;
- not attentive to addressing the issues raised by the proliferation of some content on the Web that would be legally actionable in an earlier era, such as mass sharing of copyrighted materials, which undermines systematic debate of appropriate remedies; and
- focused too narrowly on policies explicitly designed to protect or constrain freedom of expression, when the relevant legal and regulatory environment is much broader.

There are several factors that both limit the potential usefulness of research in this area and make it difficult to undertake. One such factor is technologically-deterministic optimism about the impossibility of controlling expression on the net: it is simply very hard to measure who has access to what information online as it can be accessed in so many different ways. Another is the relatively recent advent of truly global communication networks and services, particularly the worldwide diffusion of the Internet and mobile communications. Most discussion over the past decades focused on national policies affecting mass media which were typically either more local or more national in their focus, reach and governance. In comparison, the Internet is a far more recent phenomenon, still reaching only a quarter of the world's population by 2009, and is clearly not bound by the same jurisdictional limits.[8]

Another factor has been the depth of controversy surrounding discussions of global media and information flows, epitomized by the divisions created by the MacBride Commission and its report (see Box 1.1). The global significance of international news agencies and the press and mass media, along with the

emergence of new media, created a division between advocates of freedom of expression, such as representatives of the press in the most developed nations, versus advocates of efforts to balance the global flow of information, such as by redressing inequities between the developed North and the developing South. Critics have called into question basic assumptions about the primacy of freedom of the press, for example, questioning whether these principles undermined the development of a more diverse media landscape, such as by enabling greater dominance of global media firms or the dominance of Western media messages – creating a new era of cultural 'media imperialism' (Herman and McChesney 2001).

At times, debate between the advocates of the free flow of information and communication clashed with advocates of the NWICO in ways that made disinterested academic research difficult to marshal. Each camp sought support for its own position in what at times became an ideologically fraught, and correspondingly less academically reasoned debate.

Nevertheless, the MacBride report acknowledged the importance of freedom of expression, properly balanced with the laws and cultural and political-administrative traditions of nations, arguing that:

> 'It is widely recognized that freedom must be reconciled with an obligation to obey the law and must not be exploited to injure the freedom of others; also that the exercise of freedom has a counterpart which is the need to exercise it with responsibility, which in the field of communication means primarily a concern for truth and the legitimate use of the power it conveys. We need to ask moreover, on what grounds a claim for freedom is being made. The freedom of a citizen or social groups to have access to communication, both as recipients and contributors, cannot be compared to the freedom of an investor to derive profit from the media. One protects a fundamental human right; the other permits the commercialization of a social need. Yet when all these reservations are made, the principle of freedom of expression is one that admits of no exceptions, and that is applicable to people all over the world by virtual of their human dignity.' (ICCP 1980: 18).

The skepticism of the McBride Report is useful to revisit in the 21st Century, in noting that: '… as technology advances, the essential consideration at every stage should be that its progress is put at the service of better understanding between peoples and the furtherance of democratization within countries and not be used to reinforce vested interests of established powers.' (ICCP 1980: 80). In fact, we would go further in arguing that while freedom of expression should be viewed as a fundamental right, it needs to be seen in the larger context of competing values and interests. Equality and diversity of expression are a subset of a wider range of values and interests critical to understanding the key values that support freedom of expression and also those that are putting it at greater risk as we head into the second decade of the 21st Century. That is why it is necessary to look at the wider, developing ecology that is reshaping freedom of expression in the network society, but without deflecting attention from protecting this core value.

2. The Ecology of Freedom of Expression

Freedom of Expression: Foundations in Human Rights

The principle of Freedom of Expression is based on internationally recognized laws and standards for human rights (Box 2.1), such as the Universal Declaration of Human Rights (UDHR). Other regional human rights instruments address the issues of freedom of expression and privacy such as in the African Charter on Human and People's Rights[9]. Additionally, national or regional conventions are implemented to transfer these principles into national law and ensure freedoms and rights for residents and citizens.

Across Europe, the most relevant basis for freedom of expression and free speech comes from the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), along with the EU's Charter of Fundamental Human Rights. While the ECHR guarantees everyone the freedom to hold opinions and to get and pass on information and ideas, it also allows a number of qualifications, stating that these rights:

> '…may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.'[10]

Box 2.1. International Guidelines on Freedom of Expression.

Internationally Recognized Standards for Human Rights:

- Universal Declaration of Human Rights);
- International Covenant on Civil and Political Rights (ICCPR);
- International Covenant on Economic, Social and Cultural Rights (ICESCR).

Other Regional Human Rights Conventions:

- European Convention, implemented by the European Court of Human Rights;
- Charter of Fundamental Rights of the European Union[11];
- American Convention, implemented by the Inter-American Court of Human Rights and Inter-American Commission; and the
- African Charter on Human and People's Rights, under the Organization for African Union, and implemented by the African Commission on Human and People's Rights.

In the United States, Freedom of Expression is enshrined in the First Amendment to the US Constitution as part of the Bill of Rights, and upheld in more absolute terms relative to most other nations and regions. The rights

include freedom of assembly, freedom of the press, freedom of religion and freedom of speech such that:

> 'Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.'[12]

The African Charter on Human and Peoples' Rights differs from the protection afforded by other treaties as it does not explicitly include a right to hold opinions, but simply the right to receive information and to express and spread their opinions within the bounds of the law.[13] In addition, within the charter, freedom of expression is subject to the general restriction, which requires the individual to exercise protected freedoms 'with due regard to the rights of others, collective security, morality and common interest.'[14]

Formal constitutional or legal guarantees provide protection for freedom of expression in much of Asia. Examples include Article 35 of the Constitution of the People's Republic of China, Article 19 of the Indian Constitution, and Article 19 of the Constitution of Pakistan. Similar guarantees exist in the constitutions of most other Asian countries, with notable exceptions, such as the Union of Myanmar (Burma) and the Democratic People's Republic of Korea (DPRK).

A Right to Freedom of Connection

A few countries have formally recognized the importance of the right to freedom of connection. In June 2009, the French Constitutional Council ruled that the freedom to access 'public online communication services' was a basic human right[15] as it struck down France's three strikes (HADOPI) law (Bremner 2009). This law was designed to cut Internet access to users who continued to illegally download copyright material after two warnings. The same year, the Spanish government announced that its citizens would have the legal right to buy broadband Internet at 1mps, starting in 2011 (Morris 2009). Then in July 2010, Finland was recognized for being the first country in the world to pronounce broadband Internet a fundamental human right (Finnish Ministry of Transport and Communications 2010).

Following these examples, Costa Rica's constitutional court ruled in September 2010 that the Internet was also a fundamental right for its citizens, and mandated the government to provide universal access for all (Argüero 2010).[16] Estonia[17] and Greece[18] were amongst the first countries to stipulate that the State has legal obligations to provide access to electronic information and services for its citizens (Anestopoulou and McKenna 2001; Woodard 2003). These countries have made access to the Internet a basic fundamental right since the early 2000s.

Debate around the right to Internet access is increasingly growing amongst governments at all levels around the world. The Argentinean province of San Luis passed a law in 2010 which guaranteed all its citizens the right to free

Internet access[19], while the idea is being discussed by Kurdistan Regional Government's Department of Information Technology (Sutton and Clarke 2010).

A Right to Freedom of Information

As well as protecting freedom of expression, many states also provide legal guarantees for a right to freedom of information. Such rights ensure that citizens have the right to access information about how government operates, and in many cases they also impose duties on government to be transparent in operation, providing 'open records' of publicly accessible data. In so far as freedom of expression is deemed to be one of the fundamental civil rights supporting democratic processes, freedom of information is required in order to ensure that citizens can vote in an informed way, and that they can hold their governments accountable through public scrutiny.

The Ecology of Games: A Perspective on the Larger Context

The primary theme of this report is that it is helpful to broaden the context in which 'freedom of expression' is conceptualized. Not only does the pursuit of other values shape freedom of expression, but also the pursuit of freedom of expression can serve a variety of other values and interests, from democratizing communication to reinforcing vested interests, as highlighted by the controversies surrounding the NWICO. A framework of value for this purpose is based on the concept of an 'ecology of games'.

The idea of an 'ecology of games' (EoG) was introduced in local community studies within the political sciences during the 1950s (Long 1958). The concept was used to focus on a key weakness of dominant elite and pluralist perspectives on community power, arguing that few actors sought to control communities *per se*. Instead, actors sought to achieve a wide array of more specific objectives, from making their neighbourhood safer to enhancing the quality of schools to being elected to office. That is, there exists an ecology of actors, each pursuing particular objectives, and each making choices in the pursuit of those objectives that shape the development of a community. From this perspective, community development is a largely unplanned process driven by the unanticipated interactions of multiple players or stakeholders within overlapping 'games'. The unfolding history of such separate but interdependent games is then driving the evolution of local communities.

The use of the concept of 'games' is not meant to trivialize their importance. Games have a set of objectives, rules, prizes and players. Likewise, actors in public policy and regulation also have objectives, and compete or cooperate with others to achieve their objectives under a set of rules. Success can also mean that they are rewarded – there are prizes. However, the games of policy and regulation are different from parlour games in that their outcomes will shape critical aspects of everyday life and work, such as freedom of expression.

A New Framework: the Ecology of Freedom of Expression

The ecology of games perspective has been refined and developed in applications to the study of information and communication technologies and policies.[20] One contribution of this report is to provide a new perspective on the study of freedom of expression, by viewing these freedoms as the outcome of an ecology of choices made not only about freedom of expression, but also a variety of other objectives. Table 2 illustrates how the wide range of separate but interrelated goals being pursued by a variety of different actors (governments, NGOs, industry), employing an array of strategies, might influence the state of freedom of expression on the Internet.

In some cases, actors, such as those from civil society, are explicitly seeking to achieve greater freedom of expression, but others are focused on censoring expression, such as through the use of Internet filtering, the censorship of news and mass media, or efforts to silence journalists or bloggers. More indirectly, some actors are focused on quite different goals altogether, such as protecting children from harmful content, protecting their own reputation, or even promoting the vitality of an economy. The more the Internet has become central to communication, the more it has been a focus of the strategies of multiple actors in achieving their various goals, which explains the wide variety of policy areas listed in the table below.

Table 2. The Ecology of Freedom of Expression on the Internet

Categories	Objectives Defining Choices in Games
Digital Rights	Access – Freedom of Connection
	Freedom of Expression
	Censorship
	Equality, e.g., Media Literacy and Skills
	Freedom of Information (FOI)
	Privacy and Data Protection
Industrial Policy and Regulation	Intellectual Property Rights (IPR): Copyright
	IPR: Patents
	Competition
	Technology-led industrial strategies
	ICT for Development
User-Centric	Child Protection
	Decency: Pornography
	Libel: Defamation
	Hate Speech
	Fraud
Internet-centric	Internet Governance and Regulation
	Domain Names and Numbers
	Standard Setting: Identity
	Net Neutrality
	Licensing, Regulation of Internet Service Providers

Security	Secrecy, Confidentiality
	Security against malware, such as spam and viruses
	Counter-Radicalisation
	National Security, Counter-Terrorism

The following sections of this report will develop some of the key goals, actors, and strategies underlying the objectives in Table 2. This is not intended to be an exhaustive or detailed survey, but should be sufficient to show how laws and regulations in many of these areas are indeed involved in the larger ecology that is shaping freedom of expression on the Internet. As said decades ago, by the MacBride Commission (ICCP 1980: 93), the new technologies:

> 'offer considerable potential for diversifying messages and further democratizing communication. However, realizing or rejecting this potential depends, of course, on the economic, social and political choices that must be made.'

This conceptual framework seeks to identify the many political choices that are being made about law and regulation in ways that will realize or restrict the expressive potential of the Internet.

3. Connecting to the Internet: Reshaping Access

Law and Regulation Underpinning Internet Diffusion

Legal and regulatory initiatives have underpinned increasing worldwide access to the Internet and the information, communication and services that it enables. The Internet's worldwide diffusion has not been the inevitable outcome of the technology, but of a series of technological innovations shaped by policy and practice.

For example, the Internet was developed early on as the ARPANet (Advanced Research Projects Agency Network), supported by funding from the US Department of Defense. However, it was developed within universities and research institutions primarily as a tool for scientists to share computing resources, not as a tool for national defence.[21] It was born therefore in a culture of relatively free, open and trusted communication. This did not mean that abuses of this freedom did not occur. There were problems even early on within universities of individuals, such as a disgruntled student sending hate mail, but such problems were relatively easy to deal with by institutions that could identify the offending student or staff in due course and take remedial actions, such as suspending their network privileges for a period of time. Similar practices applied to the Internet today would be less feasible and more controversial as this platform has become more central to all forms of communication and information access.

Second, well before the commercial development of the Internet, governments recognized that computer-based communication systems, such as videotext in the late-1970s, and 'multi-media computers', were significantly different from the traditional media of broadcasting, telecommunication and print (Pool 1983). The regulatory regimes developed for the traditional media did not apply well to the 'new media'. Moreover, as new media were widely viewed as key to the future of communication, nations wanted to foster innovation in this area as a driver of new industry and economic development. The unique features of new media and the industrial policy goals associated with them led many governments to avoid regulation and not control content on new media, and later on the Internet. In fact, efforts to encourage new media developments extended to not taxing online purchases, and public investment in pilot projects.[22] An exception is the parallel rise of policy on privacy and data protection, such as with the European Commission's Data Protection Directive of 1995. While this directive pre-dated widespread understanding of its potential to conflict with aspects of new Internet applications, such as social media, privacy and data protection was pursued as a separate set of goals and objectives in a broader ecology of games.

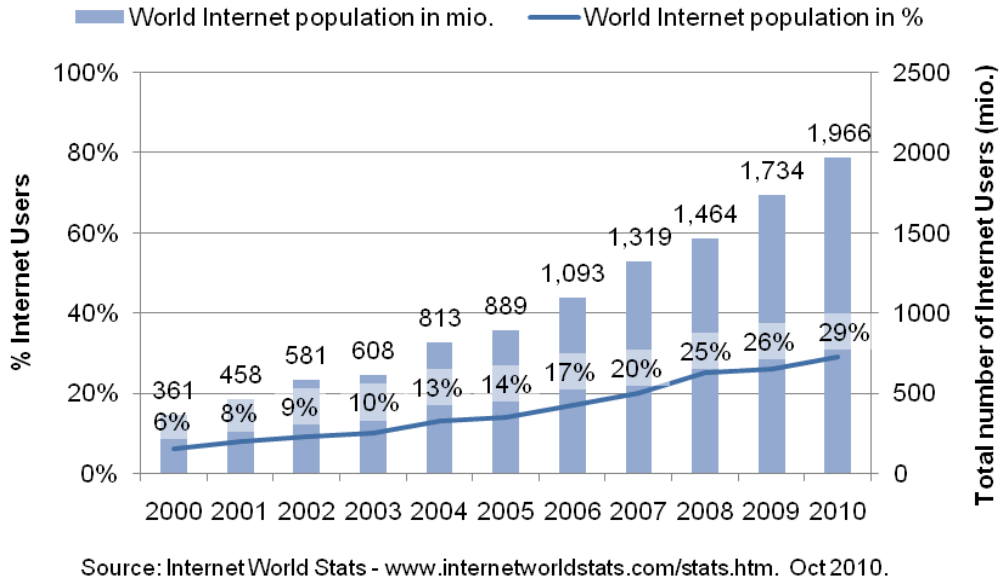
There have been many subsequent attempts to regulate data communication, largely to protect telecommunication firms, such as by legally prohibiting voice communication over computer-based networks. The diffusion of 'Voice over IP' (VoIP) services, such as the beta version of Skype, launched in 2003, has been possible because they are not legally prohibited in many nations.[23] That said, in many countries, such as where incumbent telecommunication providers have monopolies, VoIP services, such as Skype, have been blocked. This is a common practice in many African countries and other developing nations that have depended on the general revenues generated by telephone companies, but with a cost to economic development more generally. Indeed, many rapidly developing nations have been convinced of the value of liberalizing telecommunications in ways that support the Internet, such as China, which has used the Internet as a means to support the economic development of key regions (Qiu 2009).

In such ways, government policies have incentivised the development and diffusion of the Internet throughout its history as a means for enhancing technological innovation in communication and information technology and services. This is an element of industrial policy in that it supports the development of not only new information industries and businesses, but also enables innovation in all other sectors of society, from large industrial firms and agricultural enterprises, to the household, who find more efficient ways to use information and to communicate in everyday life and work. Economic development is therefore supported by the use of ICTs, rather than just their production (Baer 1996). But there is a potential from under- or over-regulation that might undermine the vitality of the Internet and its global diffusion.

Access to Technologies of the Internet

One of the most positive developments shaping the role of the Internet in opening up a new channel of expression has been its continuing pace of worldwide innovation and diffusion. By 2009, over one-quarter (26 percent) of the world's population had access to the Internet, growing from less than ten percent (6 percent) in 2000 (Figure 1). This corresponds to over 1.9 billion users by 2010 (Figure 1).

Figure 1 Worldwide Internet Diffusion of the Internet: Number of Users and Proportion of Users by World Population[24]



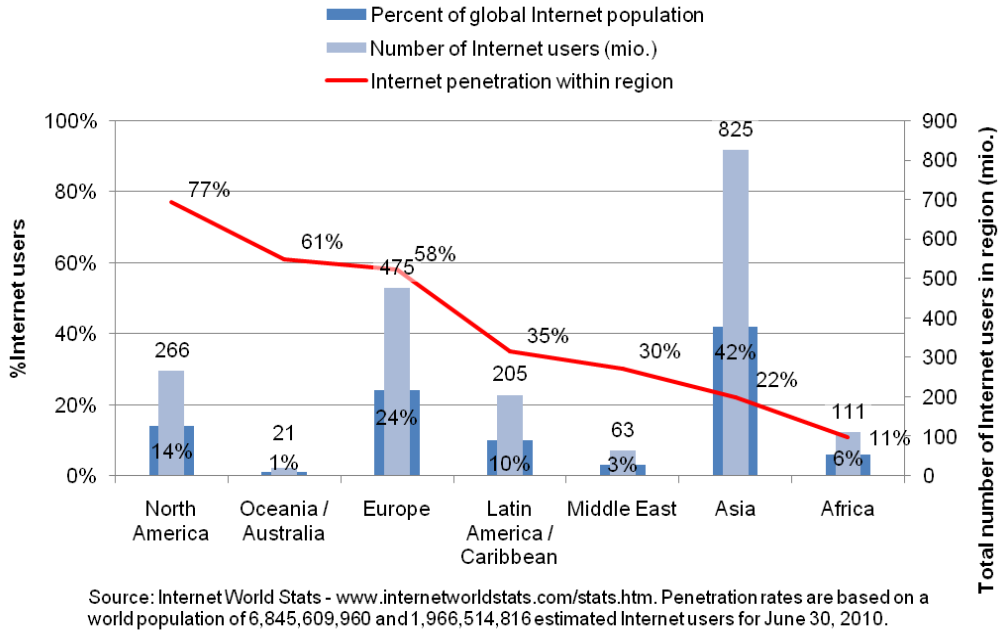
Source: Internet World Stats - www.internetworldstats.com/stats.htm. Oct 2010.

Internet diffusion has reached almost every region of the world with the exception of Africa, which has remained comparatively low in levels of Internet access at below 10 percent (Figure 2). In general, Internet diffusion remains varied by region on at least two major dimensions, which might be called 'penetration' and 'throw weight'.

Figure 2 lists major regions ranked by the proportion of the population that use the Internet – their levels of penetration in 2009. As shown in Figure 2, Africa has the lowest level of Internet penetration at about 6 percent, followed by Asia, the Middle East, Latin America and the Caribbean, Europe, Oceania and Australia, and finally North America, which has the highest proportion of its population online at over three-quarters (77percent) of the population. There is a substantial gap between Europe, with just over one half of the population online, and North America, as well as between North America and Oceania and Australia, a region closer to 60 percent. However, even in Africa, with the lowest level of penetration, the arrival of submarine fiber optic links, and the diffusion of mobile communication, promise to enhance Internet access in the coming years. Also, by 2010, mobile communication reached nearly 80% of the world's population, and is converging rapidly with Internet

communication in ways that will help diminish, but by no means erase, the divide across world regions.

Figure 2 Regional Diffusion of the Internet: Number of Users and Proportion of Users by World Regions

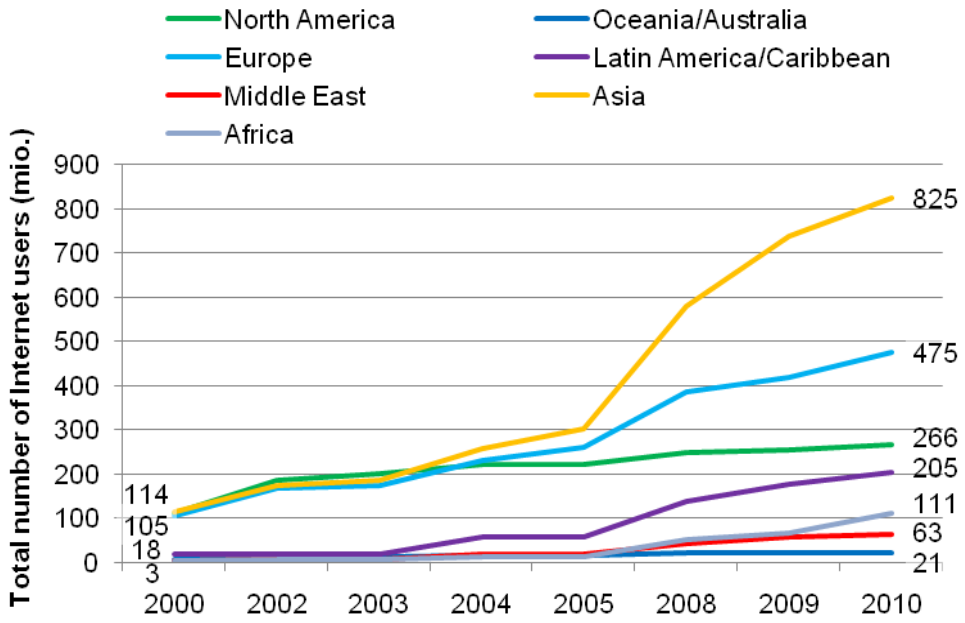


Source: Internet World Stats - www.internetworldstats.com/stats.htm. Penetration rates are based on a world population of 6,845,609,960 and 1,966,514,816 estimated Internet users for June 30, 2010.

Figure 2 also shows that while penetration rates are low in Asia, at less than 20 percent, its Internet users make up the largest proportion of the total number of Internet users online, accounting for 42 percent of the global Internet user population. By 2010, there were more Internet users in China than there were people (on or off the Internet) in the United States. Asia is clearly developing the greatest throw-weight online of any region in the world.

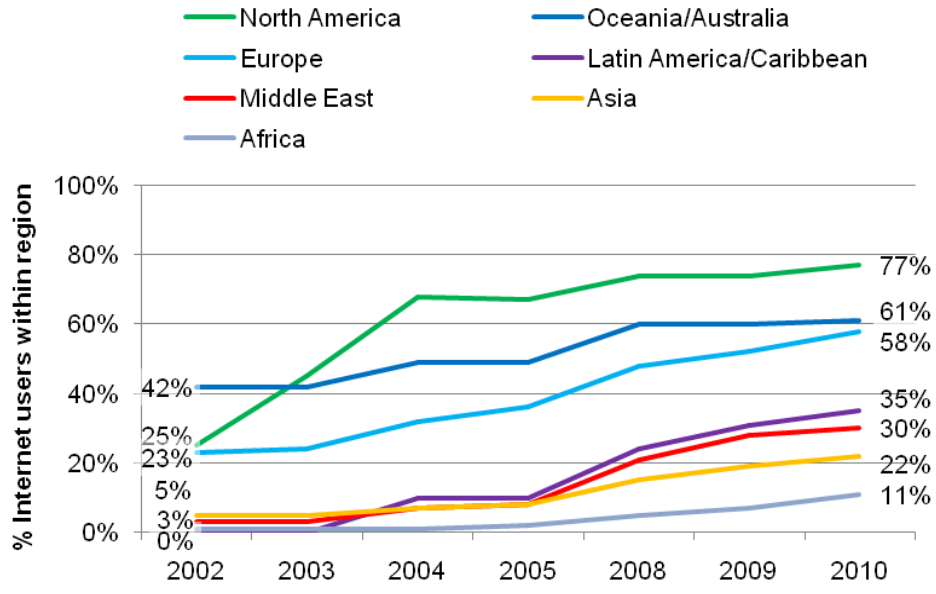
Figures 3-5 vividly illustrate the rise of Asian countries in the world's Internet population. For example, Figure 3 shows that diffusion in North America has plateaued since 2002. Europe may also have hit a plateau since 2008, but the number of Internet users in Asia continues to climb – and very rapidly. The leveling of diffusion in North America and Oceania/Australia is even more obvious when looking at the percentage of Internet users over time (Figure 4).

Figure 3. Total Number of Internet Users within Regions.



Source: Internet World Stats - www.internetworldstats.com/stats.htm. Oct 2010.

Figure 4. Percentage of Internet Users within Regions.

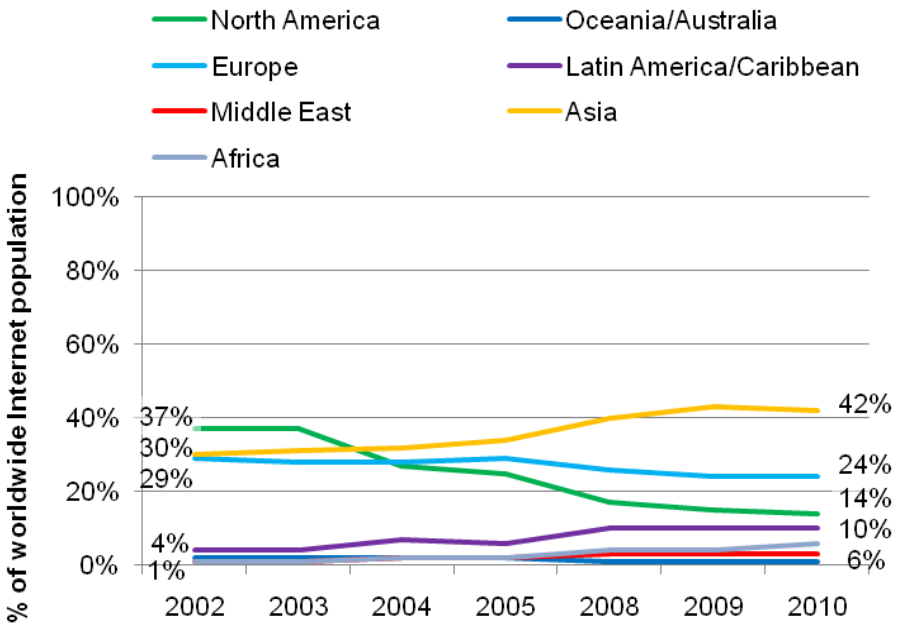


Source: Internet World Stats - www.internetworldstats.com/stats.htm. Oct 2010.

The impact of these regional changes in Internet adoption is best summarized by Figure 5, which shows North America declining from the largest plurality of the Internet population to falling below Europe and Asia. Europe is now also declining in its thro-weight online, relative to Asia. These figures dramatically illustrate a global shift in the centre of the Internet's gravity. Asia is replacing

North America and Europe as the dominant presence on the Internet, constituting an increasingly large proportion of the world Internet population, and the implications of this development for freedom of expression online have yet to become clear.

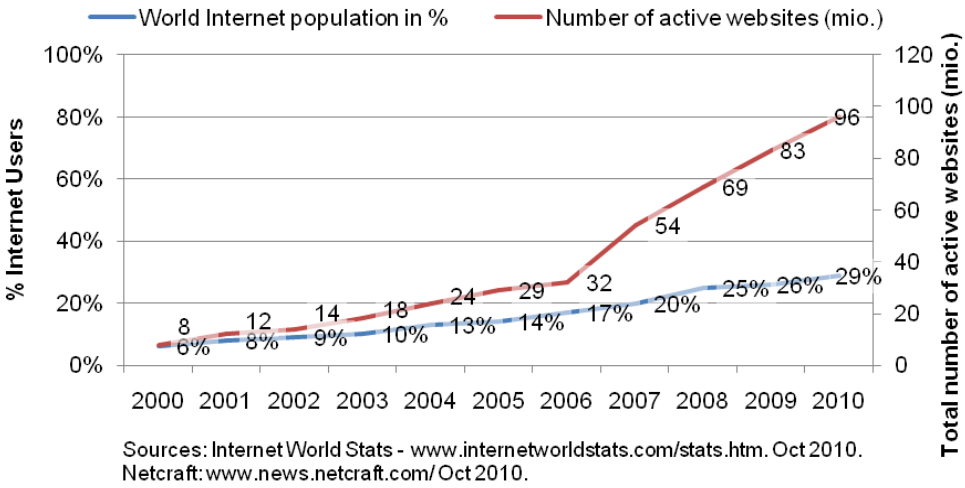
Figure 5. Percentage of Worldwide Internet Population



Source: Internet World Stats - www.internetworldstats.com/stats.htm. Oct 2010.

Finally, while the growth in Internet penetration appears gradual on a global scale, compared for example to that of mobile telephony, content continues to expand at a fast pace (Figure 6). The number of active websites increased significantly after 2006 and appears to be growing steadily, creating a virtuous cycle of more content generating more use and more use generating more content.

Figure 6. Percentage of Worldwide Internet Usage by Number of Active Websites



Sources: Internet World Stats - www.internetworldstats.com/stats.htm. Oct 2010.
Netcraft: www.news.netcraft.com/ Oct 2010.

Equality: Access to Skills and Technologies

Previously, skills and infrastructures necessary to produce and disseminate content for many media, such as the press, radio and television, were highly centralized. The potential of the Internet and the advances of related technologies such as video, Web 2.0 applications and mobile devices have enabled a more decentralized production of content. However, access to the Internet does not automatically translate into its use for the production of new content. Most users are primarily consumers of Internet services, rather than producers of original content. The potential of the Internet, like other ICTs, to 'reconfigure access', is not always realized.

This is one reason why many nations are aggressively pursuing initiatives designed to enhance the proficiency and literacy of Internet users. This could not only enable more people to benefit from the vast array of information online, but also allow them to contribute original and local content to the world wide web. The McBride Commission might have recognized the long-term potential of the new technologies to reconfigure global information flows, but this potential has never before been as technically feasible as it is today; ensuring the appropriate skill levels remains a major challenge.

In contrast to the mass media of film and television, the Internet has a greater potential to transform the geography of production and consumption, enabling a more decentralized production and more diverse flows of content around the world. However, it could also further centralize content production, given the concentration of media skills in major centres, such as Los Angeles and London. Research on the geography of content production and consumption is in its early stages, but it is a clear priority of research on the Internet.[25] The key question is whether or not the Internet is enabling a more diverse and

decentralized production of content, and will users take advantage of this potential? Increasingly, as access becomes more widespread, debate will turn back to the themes that gripped mass media studies around worldwide information flows, such as those highlighted by the McBride Commission.

4. Technologies of Disconnection

The most extensive empirical research project which examines government filtering and website blocking suggests that these practices have increased since 2002, when this project began (Deibert et al 2008, 2010). These trends are supported by related research from organizations focused on freedom of expression, including Freedom House (2009) and Reporters without Borders (2010).

Filtering

In parallel with advances in technology underpinning greater access to the Internet and mobile communication technologies, there have been innovations in technological approaches to controlling the flow of information over these networks. This has been driven by the need to maintain and improve the quality and security of services, such as by screening out spam email and viruses, but also by efforts to block unwanted content as judged by individuals, parents, NGOs, corporations or governments. Regulation of Internet content is enabled by these technological approaches, which can be implemented at several different levels (Box 4.1). As information and communication flows online, it may use several Internet related protocols and services and pass through various points in the Internet network as well as the end user's device. As a result, filtering methods can be applied at various points throughout the network. Most concern is focused on state- or government-sponsored or enforced filtering, but even when state-mandated, it can be implemented at different levels and by various different parties such as individuals, institutions or service providers. Generally, those concerned about the civil liberties of Internet users want filtering decisions to be made at the lowest possible level – as close as possible to the individual user.

Box 4.1. The Locus of Filtering Technologies.

The most common points at which filtering can be applied include:

- Internet Service Providers: ISPs are often mandated, encouraged, or incentivised to filter illegal or immoral content, or prevent search results from specified Websites, by a regulator or other agency authorized by a government with jurisdiction over their activities. They also routinely filter spam and attempt to prevent infection by malware for reasons of stability and user protection.
- Gateways to the Internet Backbone: State-directed implementation of national content filtering schemes and blocking technologies may be

carried out at the backbone level, often with filtering systems set up at links to the Internet backbone, such as international gateways in order to eliminate access to content throughout an entire country.
- Institutions: Companies, schools, libraries and households can filter on the basis of their own criteria or on behalf of state authorities
- Individual Computers: filtering software can be installed on individual computers, such as a personal computer, that restricts the ability to access certain sites or use certain applications.
- Law Enforcement: actions taken against users who engage in unlawful file sharing of music, malicious hacking, fraud, etc.

Adapted from: Zittrain (2006) and Callanan et al (2009).

Box 4.2. Deep Packet Inspection (DPI)

Deep packet inspection is the use of computer systems that can inspect packets sent over networks using the Internet Protocol suite in ways that enable a third party, not the sender or receiver, to identify particular aspects of the communication. Inspection is done by a 'middle-man', not an endpoint of a communication, using the actual content of the message. For example, ISPs can apply this technology for the lawful intercept of messages on public networks to determine if customers are using the network for unlawful purposes or purposes that violate their user agreements. Governments in North America, Asia and Africa use DPI for various purposes such as surveillance (Nelson 2006) and censorship (Wagner 2009). DPI can serve as a 'one for all' solution to monitor or regulate traffic and communication elements: e.g. the interception and logging of Internet traffic, enforcement of copyright, prioritizing limited bandwidth, and tracking users' behavior. DPI thus can serve interests of many stakeholders:

- government agencies and content providers, who are interested in the monitoring and filtering of information flows (political control);
- network operating staff, who have to deal with malware and bandwidth-hungry applications (technological efficiency);
- vertically integrated ISPs that want to create additional revenues or protect them, e.g. through preventing the Internet from cannibalizing their telephone- or video-on-demand revenues (economic interests).

See: Ralf Bendrath: DPI as an Integrated Technology of Control – Potential and Reality http://dpi.priv.gc.ca/index.php/essays/dpi-as-an-integrated-technology-of-control-%E2%80%93-potential-and-reality/

Most forms of filtering require some inspection of the content of a message, which could be derived from the identity of the source, header information, for example, or the actual content of the message, such as the words, strings of words or images in the message or on the Web site. Increasingly this involves what is called 'deep packet inspection' (Box 4.2).

There are also a number of approaches to filtering, such as blocking an IP address, a Domain Name System (DNS) name, a Universal Reference Identifier (URI), or keywords (Box 4.3). Each involves somewhat different technical methods. Keyword filtering requires more advanced techniques to be well targeted, but it is being used by a growing number of countries.

Box 4.3. Approaches to Blocking.

- Internet Protocol (IP) blocking, by screening particular IP addresses;
- Blocking, or manipulating, DNS information, which involves falsifying the response that is returned by a DNS server;
- Universal Reference Identifier (URI) blocking, which screens out specific resources from a specific Web site; and
- Keyword blocking, which denies access to websites based on the words found in pages or URIs, or blocks searches involving blacklisted terms. Advances are enabling increasingly dynamic, real-time analysis of content, but it is not yet in wide use.

Filtering methods often use some kind of blacklist (or 'allow' lists) that are configured to pass traffic by default unless it contains certain content, names, or keywords which are on the list. Filters are also often adjusted as information is passed on from law enforcement investigations or consumer complaints. If blocking takes place within a certain network, such as within a company, the network administrator is often the person who manually defines the filtering. In contrast, many defence filters or virus scanners often use pre-defined criteria to filter the content automatically.

Many contemporary filtering techniques are blunt instruments, often leading to some level of over- or under-blocking. For example, it is almost impossible to block only the content aimed for without unintentionally blocking other material.

Counter-measures for Filtering

Many technologically savvy users can find alternative methods to access blocked content. However, for most people, blocking is an effective means for preventing access. Nevertheless, as filtering or blocking content does not erase the original content, some users can still access the content by using other connections for which access has not been blocked, creating a cat and mouse game between actors seeking to gain or block access to particular content. The fact that websites are not removed, but blocked, can mean that, for example in the case of child protection, the content has not been destroyed, but it has been made invisible for most non tech-savvy users.

The Arrest of Journalists and Bloggers

Control is not limited to filtering or censorship. Recent years have seen an increase in a wide variety of threats to freedom on the Internet, such as an increase in arrests of bloggers and Internet users. The Committee to Protect Journalists found that in 2008, there were, for the first time, more jailed 'cyber-dissidents', such as bloggers, than traditional media journalists.[26] The arrest or detention of content producers, such as journalists or bloggers, or users, such as those who are accessing or consuming unlawful or otherwise targeted material, is one of the most traditional forms of content control. In doing so, surveillance and monitoring methods are often used to identify users or producers (see Boxes 4.4, 4.5 and 4.6).

Box 4.4. A Twitter-Based Arrest in the USA.

During the Group of 20 summit in Pittsburg, Pennsylvania, in October 2009, close to 200 arrests were made during demonstrations involving up to 5,000 protesters. One arrest made at a Pittsburg motel by Pennsylvania State Police was of a 41 year old New York social worker, named Elliot Madison, for being part of a group that posted messages on Twitter that were designed to help protesters at the G-20 summit 'avoid apprehension after a lawful order to disperse'. He was found with computers and police scanners while using the micro-blogging service Twitter. According to available accounts, FBI agents later executed a search warrant at his home in Jackson Heights, Queens, New York, for 'evidence of federal anti-rioting law violations'.

Source: Moynihan (2009) and Valetk (2009).

Box 4.5. Twitter in the Iranian 2009 Election Protests.

In the midst of protests surrounding the contested 2009 election results in Iran, the Internet, and Twitter in particular, was claimed to have played an important role in organizing and supporting the protests on the streets of Tehran. Overall, there is little doubt that Twitter and videos posted on the Web played a significant role in providing a means for individuals in Iran to communicate with one another, but most often via the world outside Iran. The main role of Twitter was as a tool for the Iranian Diaspora to relay protest news to the international media, which in turn became a significant factor in shaping and informing developments on the ground.[27]

That said, English language Twitterers from the Iranian Diaspora became bridges between events in Iran and the 24-hour English news cycle, which followed Twitter feeds during this period. A few weeks before the election CNN appointed its own 'Twitter Correspondent'. Andrew Sullivan coined the term 'twitter revolution' two days after the election and played a key role in promoting the 'Tweeting for Iran' campaign. Later, the State Department also fueled the attention surrounding Twitter by asking Twitter to postpone their routine maintenance as there was a Twitter revolution going on in Iran.

Although Twitter might not have played a critical role in shaping the flow of

information into Iran or being used as a tool by the opposition to organize themselves during the unrest, the episode introduced Twitter to many individuals inside Iran and as a result there are many more users of Twitter inside Iran after than before the protests. Even so, 'Citizen Journalist' videos played an important role. The more foreign media activities were restricted, the more these citizen videos filled the void. BBC Persian TV relied on these videos for its coverage of Iran. Satellite TV stations like BBC Persian and Voice of America played an important role in informing and effectively organizing people. Defence was also very effective due to its low bandwidth and features that make its content easy to share. Most significant were human networks (there are videos of people on YouTube shouting in the Tehran metro promoting the upcoming protest gatherings). In Iran there was an alignment of old and new media, forming a cycle of technically-enabled users publishing news online and uploading video footage, outside media picking up these materials and sending them back to Iran for a larger audience, which users further disseminated through their own networks.

The counter measures used by the Iranian government to break this cycle were quite effective. On important protest days, Iranian authorities effectively pulled the plug on the Internet, introducing 60-70% packet loss into the network and closing all the major ports used by circumvention tools, making it nearly impossible for ordinary users to do anything online. On normal and non-critical days, Iran appeared to be doing deep packet inspection. On the satellite TV front, authorities jammed the signals of political Persian Satellite TV stations, forcing them to shut down or move to less popular satellite platforms. Due to heavy jamming on BBC Persian TV, HotBird and NileSat decided to stop broadcasting BBC Persian as the jamming was interfering with other channels. All of these were in addition to offline methods of shutting down, banning, arresting, and intimidating protestors.

Box 4.6. Freedom of Expression in Vietnam[28]

Dozens of dissident activists, bloggers and writers active online have been arrested by the Vietnamese government, most often for writing commentary, such as on Sino-Vietnamese relations.[29] The International PEN, Amnesty International, Asian Forum for Human Rights and Development, Reporters Without Borders, Human Rights Watch and the World Organization Against Torture have all reported severe restrictions on Internet freedom in Vietnam, with the Committee to Protect Journalists (CPJ) naming Vietnam as one of the 10 most dangerous countries to be a blogger.[30]

On its official website, the Vietnam Ministry of Information and Communications (MIC) listed as its main functions to include: "manage all types of press… including electronic and information on the [I]nternet".[31] As official media has been restricted under the Communist Party, many people have gone to the Internet to discuss controversial issues more freely (Pham 2009), leading to crackdowns utilizing Article 88 "Propaganda Against the State" and Article 258 "Abusing democratic freedoms to infringe upon the State interests" under the Vietnamese Penal Code.

In October 2009, eight Vietnamese bloggers received jail sentences, which ranged from two to six years. They were accused of disseminating anti-government propaganda under Article 88 of the Vietnamese Penal Code.[32]

Alternatives to Filtering

Government agencies have used a number of techniques to deny access or censor particular types of content that differ from content filtering. These include:

- Denial of service attacks, which produce the same end result as other technical blocking techniques - blocking access to certain websites - although only temporarily, and this is more often used by non-state actors seeking to disrupt services;
- Restricting access to domains or to the Internet, such as by installing high barriers (costs, personal requirements) to register a domain or even to get Internet access;
- Search Result Removals, by which search engine providers can filter web content and exclude unwanted websites and web pages from search results. By using blacklists, parsing content and keywords of web pages, search engines are able to hinder access. This method makes circumventing the denial of access more difficult as search engines are not always transparent about the filtering of search results; and
- Take-down of Websites, by removing illegal sites from servers, is one of the most effective ways of regulating content. To do so, regulators need to have direct access to content hosts, or the legal jurisdiction over the content hosts, or an ability to force ISPs to take down particular sites. In several countries, where authorities have control of domain name servers, officials can deregister a domain that is hosting restricted content (Deibert et al 2008).

There are, of course, other ways of influencing the content that users consume or produce which do not involve filtering technology. Content can be influenced by introducing rules, or laws, or by instilling social norms among content producers. This can be enforced by the threat of legal action, but also by social pressure for commitment.

One creative approach to addressing content concerns is to enter Internet conversations. This is an approach that is most in tune with the spirit of free expression, but only if it is transparent. For example, the US State Department has initiated an effort to respond to what they view as misinformation and inaccurate accounts of US policy and actions on Arab language blogs and Websites by commenting on the blogs, and explicitly identifying themselves as representatives of the US State Department. In many respects, this is a modern form of public diplomacy, adapted to the Web

2.0 technologies of the Internet and in keeping with open access to more diverse sources of information.

However, some regimes have increasingly resorted to guiding or influencing online discussion without being transparent, such as through the clandestine use of paid pro-government commentators or the financing of entire websites and blogs (Karlekar and Cook 2009). Freedom House (2009) pins this offence on the Chinese government for employing '50 Cent Party' commentators, Russia for using Kremlin-affiliated 'content providers', and Tunisia for using similar approaches to 'subvert online conversations'.

Governments may also seek to counter particular political movements or to guide online opinion by producing online publications or 'propaganda' such as pro-government websites. This is of course an online analogy to long-held efforts of governments to provide information over the mass media, such as the Voice of America (VOA) in the US, which has moved from radio and television broadcasting to become a multimedia source of news and information about the US. Arguably, governmental provision of information is entirely in keeping with principles of freedom of expression, as long as it is transparent and not overwhelming alternative sources of information.

As this section argues, the control of information on the Internet and Web is certainly feasible and technological advances do not therefore guarantee greater freedom of speech. There are many tools available and still more in development. The legitimacy or otherwise of this control cannot be determined without unpacking political and cultural choices about who should control what content in which ways, for what purposes, and with what level of transparency. This leads us to a consideration of the legal frameworks and motivations behind such diverse goals as censorship of political speech, copyright protection or eradication of child abuse. The next section begins this discussion by focusing on law and policy supporting freedom of expression.

5. National Practices and Trends Worldwide

International trends can be tracked on at least two different levels. One concerns the actual practices of censorship, such as Internet filtering. The other concerns public perception. Do individuals believe they are more or less free to express their opinions? This section will address both in turn.

Internet Filtering and Censorship

In the early years of the 21st century, an increasing number of governments have taken steps to block or regulate Internet access or content. This increase can be seen most clearly in the work of Freedom House (2009), based on their Global Index of Internet Freedom (Box 5.1) and the OpenNet Initiative (Box 0.5). The OpenNet Initiative reported on only a few governments documented to be blocking online content in 2002, while by 2007 they estimated that at least 40 countries used methods to do so (Deibert

et al 2008). Thus, national regulation of the Internet is taking place on a wide scale, despite ambiguity over appropriate policy and uncertainty over its implementation, and risks to freedom of expression (Deibert et all 2008; Freedom House 2009).

Box 5.1. The Profile of Global Freedom (PGF)

Freedom House is an independent nongovernmental organization, which focuses on uncovering efforts to restrict transmission of news and politically relevant communications, while acknowledging that some restrictions on harmful content may be legitimate. It compiles a profile of global freedom that indexes restrictions from both government and non-state actors. The key components of the index are access to technology as well as free flow of information and content. Each country gets scores from 0 (the most free) to 100 (the least free), which serves as a basis for an Internet freedom status designation of Free (0-30 points), Partly Free (31-60 points), or Not Free (61-100). The approach considers various factors that could affect levels of Internet freedom, including dynamics within each country, both in terms of changing methods of restriction as well as changes over time. Their 2009 report on freedom on the Internet provides an overview on strategies and trends, such as the 'outsourcing of censorship' to private companies and the use of surveillance by state actors. The index covers both more repressive countries such as China and Iran and more liberal democratic nations such as India and the United Kingdom, and finds some degree of Internet censorship and control in all 15 nations studied.

See: Freedom House (2009) and online see: http://www.freedomhouse.org/uploads/specialreports/NetFreedom2009/FOTN%20Overview%20Essay.pdf

Studies by the OpenNet Initiative offer some of the most extensive surveys of Internet filtering (Deibert and others 2008, 2010), along with detailed country by country overviews. The European Digital Rights website[33] also provides an overview on filtering tendencies and country cases.

It is often thought that content control systems are only established in undemocratic countries or by authoritarian regimes wishing to control political speech or criticism. In fact, content control measures have become more prevalent around the world and are often undertaken for a wide variety of reasons, often with very good intentions. Our own meta-analysis of existing surveys illustrates that many nations are likely to exercise some level of control, but that only a minority exhibit pervasive levels of censorship (Table 4).[34] Australia, Canada, China, Finland, France, Germany, Japan, Kyrgyzstan, Saudi Arabia, the UK, the US and Uzbekistan are just a few countries who have implemented national filtering systems or have presented legislation to approve filtering practices.

In democratic societies, issues of copyright infringement, hate speech, defamation, privacy protection, and child protection are at times a basis for Internet filtering or other content control. Clearly it could be argued that filtering for such purposes does not represent as significant a threat to freedom of expression as the deliberate blocking of political speech or information and communication for certain social minority groups. Others, who see freedom of expression as an absolute right of fundamental importance might disagree. This report does not seek to make such value judgments and instead seeks to expose the extent of the legal and regulatory trends affecting freedom of expression online. As such, it should be noted that the meta-analysis presented below (Table 3) measures only the extent of filtering rather than the significance of the blocked material.

Table 3. Meta-Analysis of International Surveys of Filtering

Country	**OpenNet Evidence of Filtering Levels**								**Freedom House**	**Overall Rating**
	Political		Social		Security		Overall			
	2007	2009	2007	2009	2007	2009	2007	2009		
Armenia	-	M	-	L	-	L	-	M	-	Medium
Australia	-	NE	-	M	-	NE	-	M	-	Medium
Azerbaijan	L	L	NE	L	NE	NE	L	L	-	Low
Bahrain	M	-	L	-	NE	-	M	-	-	Medium
Belarus	NE	L	NE	L	NE	L	NE	L	-	Low
Brazil	-	-	-	-	-	-	-	-	Low	Low
China	H	H	M	M	H	H	H	H	High	High
Cuba	-	-	-	-	-	-	-	-	High	High
Egypt	-	NE	-	NE	-	NE	-	NE	Medium	Medium
Ethiopia	M	-	L	-	L	-	M	-	-	Medium
Estonia	-	-	-	-	-	-	-	-	Low	Low
France	-	NE	-	NE	-	NE	-	NE	-	NE
Georgia	-	L	-	NE	-	L	-	L	Medium	Medium
Germany	-	NE	-	NE	-	NE	-	NE	-	NE
India	NE	-	NE	-	NE	-	L	-	Medium	Medium
Iran	H	H	H	H	M	M	H	H	High	High
Italy	-	NE	-	L	-	NE	-	L	-	Low
Jordan	L	-	NE	-	NE	-	L	-	-	Low
Kazakhstan	NE	L	NE	L	NE	NE	NE	L	-	Low
Kenya	-	-	-	-	-	-	-	-	Medium	Medium
Kyrgyzstan	-	L	-	L	-	NE	-	L	-	Low
Libya	M	-	NE	-	NE	-	M	-	-	Medium
Malaysia	-	-	-	-	-	-	-	-	Medium	Medium
Moldova	-	L	-	NE	-	NE	-	L	-	Low
Morocco	NE	-	NE	-	L	-	L	-	-	Low
Myanmar	H	H	M	M	M	M	H	H	-	High
Oman	NE	-	H	-	NE	-	H	-	-	High
Pakistan	L	NE	M	M	H	M	H	M	-	Medium*
Russia	-	L	-	L	-	NE	-	NE	Medium	Medium
Saudi Arabia	M	-	H	-	L	-	H	-	-	High
Singapore	NE	-	L	-	NE	-	L	-	-	Low
S. Africa	-	-	-	-	-	-	-	-	Low	Low
S. Korea	NE	NE	L	M	H	H	H	H	-	High

Sudan	NE	-	H	-	NE	-	H	-	-	High
Syria	H	-	L	-	L	-	H	-	-	High
Tajikistan	L	L	NE	NE	NE	NE	L	L	-	Low
Thailand	L	-	M	-	NE	-	M	-	-	Medium
Tunisia	H	-	H	-	L	-	H	-	High	High
Turkey	-	L	-	L	-	NE	-	L	Medium	Medium
Turkmenistan	-	H	-	L	-	L	-	H	-	High
UAE	L	-	H	-	L	-	H	-	-	High
Ukraine	-	NE	-	NE	-	NE	-	NE	-	NE
United Kingdom	-	NE	-	NE	-	NE	-	NE	Low	Low
USA	-	NE	-	NE	-	NE	-	NE	-	NE
Uzbekistan	M	H	L	L	NE	L	M	H	-	High*
Vietnam	H	-	L	-	NE	-	H	-	-	High
Yemen	L	-	H	-	L	-	H	-	-	High

Key: Collapsed ratings from different studies into one more general rating:

For OpenNet:
NE = no clear evidence, including 'suspected filtering';
Low = evidence of selective filtering;
Medium = 'substantial filtering';
High = 'evidence of pervasive filtering' (Faris and Villeneuve 2008: Table 1.5). Overall = highest level of filtering across categories.

For Freedom House Ratings:
Low = 10-26, rated 'Free';
Medium = 27-55, rated 'Partly Free';
High = over 55, rated 'Not Free' (Freedom House 2009: p. 20).
A '-' indicates that the country was not covered by the respective study / in the respective year.
'*' indicates that the rating for the respective country has changed from 2007 to 2009.

Of the states examined, those with the most extensive filtering practices are China, Cuba, Myanmar (Burma), Oman, South Korea, Sudan, Syria, Tunisia, Turkmenistan, United Arab Emirates, Uzbekistan, Vietnam, and Yemen. These nations fall primarily in three regions: East Asia, the Middle East and North Africa, and Central Asia. Nevertheless, there is great diversity in filtering practices within these regions. In the Asia-Pacific region, much has been written about the 'Great Firewall of China', and there is widespread agreement that China has one of the most sophisticated and pervasive filtering systems for Internet censorship.[35] Vietnam follows many similar practices. Myanmar (Burma) famously shut down the Internet in the fall of 2007, during disturbances. In South Korea, the Internet is generally free, except in the area of national security, where there are tight controls. Pakistan and Sri Lanka restrict politically sensitive sites.

Although no significant restrictions were reported in the studies used for the meta-analysis, filtering in North America and Western Europe is mostly targeted at child sexual abuse images or hate speech and propaganda (Zittrain and Palfrey 2007). Cuba is a notable exception in the region with severe restrictions on access. In Central and Eastern Europe there is high regional diversity with some states being quite open and others taking steps

to block access (Belarus and Kazakhstan compared to Turkmenistan). In the Middle East and North Africa, the blocking of websites is fairly extensive, especially in Syria and Iran. On the African continent, the lack of access to the Internet is the greatest obstacle to expression. In addition, while the Internet is only now beginning to play a major role due to financial and infrastructural constraints, Gambia and Ethiopia have already started to block sites and restrict access.

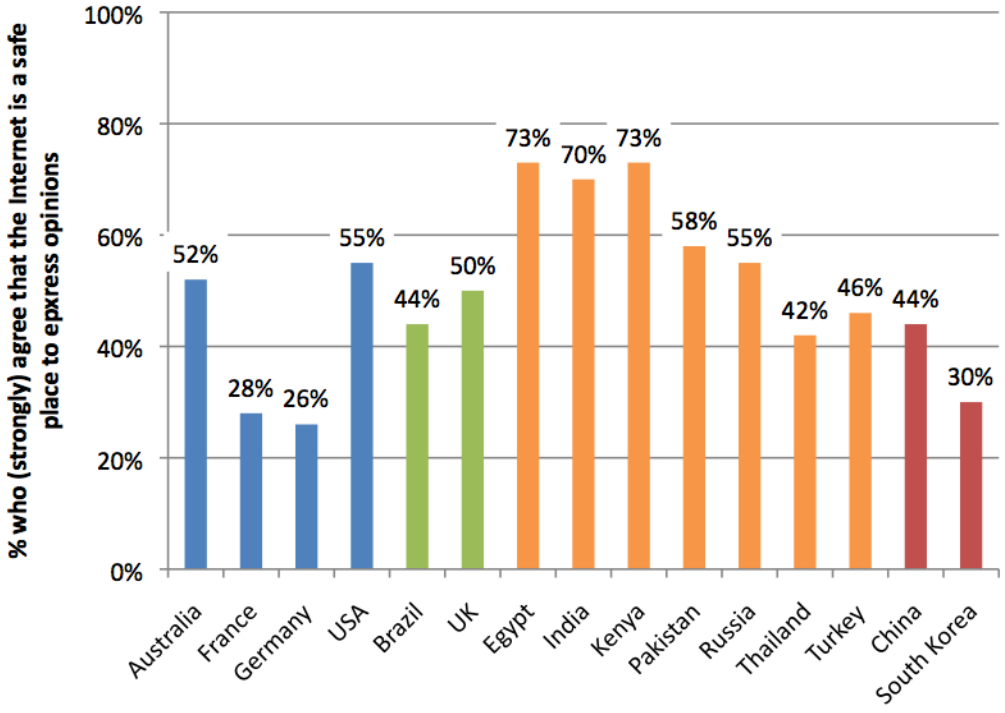
Public Opinion: Beliefs and Attitudes Concerning Internet Freedom

There is a need to continue efforts to track trends in Internet censorship and filtering, but also to more broadly assess the outcome of this evolving ecology. How can we more effectively gauge citizen experiences with respect to freedom of expression over time and across national and regional jurisdictions. Can we measure freedom of expression in more meaningful ways? Will it be possible to compare and contrast these indicators so that the world can monitor shifts in freedom of expression? For example, this collaborative project has already stimulated the development of a World Internet Policy Project (WIP2), which intends to monitor policy changes shaping the Internet worldwide. In such ways, the project aims to efficiently tap the wisdom of the wider Internet community for critical case studies, emerging legal initiatives and regulatory trends that need to be a focus of those concerned with the freedom of expression generally, and online in particular.

Separately, the BBC has conducted a global Internet survey that addresses questions relevant to these concerns (Figures 7 and 8). Most interestingly, their global survey shows that attitudes and beliefs about freedom of expression do not have straightforward associations with actual practice. Those who use the Internet, even in nations that have reputations and practices of monitoring and censorship, feel better able to express themselves, but some users in nations with more liberal democratic traditions feel restraints on expressing themselves (Figure 7). However, across the range of world cultures tapped by this survey, there was widespread support for the freedom – maybe even the right – to connect (Figure 8).

Figure 7 shows the percentage of people who strongly or somewhat agreed that the Internet is a safe place to express their opinions. This question was only asked to people who declared that they used the Internet in the last six months. Egypt, India and Kenya appear to have the highest percentages of people who strongly or somewhat agree that the Internet is a safe place to express their opinions. Those who agree the least are people in Germany and France, followed by citizens in highly filtered countries such as China and South Korea.

Figure 7. The Internet is a Safe Place to Express my Opinions[36].

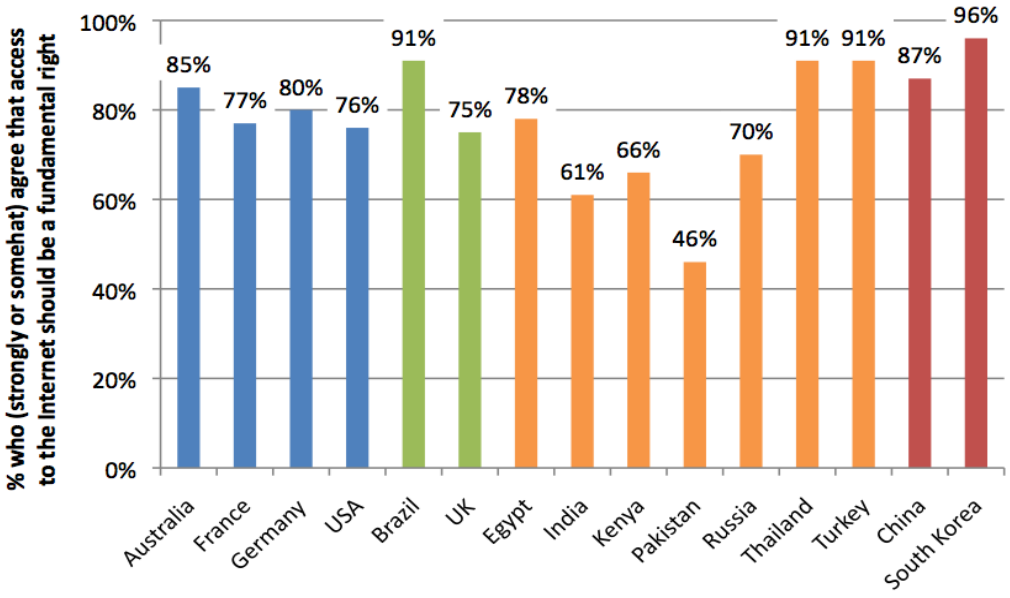


Source: BBC (2010): 15. Percentage of Internet users responding 'strongly agree' or 'somewhat agree' with the statement: The Internet is a safe place to express my opinions'.

At first glance, some of these figures may seem surprising, but it is important to note that there are several particularities limiting comparability. First, samples were not weighted to reflect the overall population of Internet users. Second, samples in some cases represented national populations and in other cases represented only the urban populations (Brazil, China, Egypt, Turkey). Methodology also varied across countries between face-to-face and phone interviews, though the methodology chosen within a country remained consistent. The sample frame also showed a few discrepancies. In most cases, people interviewed were 18 years old or older. However, there were a few exceptions, notably in Turkey where the age frame was 15+, and in Germany 16+. People surveyed in South Korea were 19 years old or more. The reason for these sample inconsistencies is likely to be tied to different national assumptions about the appropriateness of interviews with younger people. On their own, these incongruities may not make much difference, but together they can produce differences that might account for minor variations.

Despite these caveats, the BBC survey may be hinting at some important dynamics found in particular countries, such as France and Germany where fewer users agreed that the Internet was a safe place to express opinions. Recent legislation such as France's HADOPI (also known as the three strikes law), and Germany's Data Retention Law as well as Internet filtering law, might help to explain why there seems to be less faith in the Internet. In contrast, a more recent experience with Internet diffusion might explain why there's a more optimistic perspective in countries such as Egypt and Kenya.

Figure 8. Access to the Internet Should be a Fundamental Right of All People [a]



[A] Source: BBC (2010): 17. Percent who 'strongly agree' or 'somewhat agree' to the statement: 'Access to the Internet should be a fundamental right of all people.'

When looking at Figure 8, the same problems with samples apply. However, the graph indicates that in all countries except Pakistan, the overwhelming majority of people interviewed (users and non-users) agreed that access to the Internet should be a fundamental right of all people. In Pakistan, only 46% of those surveyed agreed to this statement. However, this country also had one of the highest response rates in the 'don't know/not applicable' category (23%).

The BBC survey also asked users a question related to what they thought was the most valued aspect of the Internet. On average, 'finding information of all sorts' was deemed the most important characteristic (46%) above other options such as 'interacting with people' (32%) and 'source of entertainment' (12%). Therefore, there might be a relationship between people believing that access to the Internet should be a fundamental right for everyone and that its most valued aspect is finding information.

What this graph does not show is which countries have the highest percentage of respondents who strongly disagreed that the Internet should be a fundamental right of all people. Japan had the highest percentage rate at 13% followed by Pakistan and Kenya at 11%. However what may be surprising is that, amongst the 26 countries polled, the USA (rounded up to 11%) and Canada (10%) are also among the top five countries where people most strongly disagreed that access to the Internet was a fundamental right of all people. These findings illustrate the complex relationships between government policies and public beliefs and attitudes, an area deserving further research.

6. Legal and Regulatory Protections of Digital Rights

As outlined in the previous section, many nations use content blocking and filtering to achieve a wide range of policy objectives. Most countries use some mix of existing media, telecommunications, national security, and Internet-specific law and regulation to justify restrictions on publishing, or access to online information. In this context it is important to remember that regulation often targets a particular type of action rather than a specific communication medium, addressing illegal acts regardless if committed online or offline, such as defamation or fraud. This section outlines how legal and regulatory efforts to protect a broad set of digital rights are shaping freedom of expression online.

Controlling the Internet is a fundamental aspect of 'Internet politics' (Seltzer 2008) and most countries have viewed some level of censorship as a legitimate means to protect a nation's interest, such as in online child protection (Hills 2006). However, the degree and nature of legitimate targets of online censorship can vary significantly, depending on the actor, and the cultural or political character of the state in which it occurs.

The transparency and implementation of government policy are a key problem here. Often, it is not clear from policy statements and law to what extent access to Internet material is blocked. The need for empirical studies of online filtering is a symptom of this general lack of transparency overall. In contrast, censorship of print or broadcast material in most nations is often more publicly identified and debated.

Transparency is also hampered by the fact that not all governments take responsibility for monitoring online content by directly monitoring users. An increasing number of countries, including China and Britain, have enlisted private stakeholders such as search engines and ISPs to operate as proxies (Kreimer 2006). In some cases, ISPs are strongly encouraged to adopt filtering systems (Brown 2007). In other cases, service providers simply choose to offer filtering services themselves, even if they are not directed to do so by a governmental or regulatory authority (Palfrey 2006). Where ISPs require a licence to operate, compliance is easy to understand, although such self-regulation makes accountability and transparency harder to achieve.

Table 4. Digital Rights: Stakeholders and Strategies.

Goals - Games	*Main Stakeholders*	*Strategies - Objectives*
Access – Freedom of Connection	Internet business and industries; governments; civil society advocates; producers and consumers of information and communication services	Develop infrastructures and services; media literacy and skills development; provide public access facilities; and reduce costs to access
Freedom of	Civil society and human	Challenge practices, laws

Expression	rights advocates; the press and media organizations	and regulations that impinge on free expression
Censorship	Governments and regulatory authorities; ISPs; political and interests groups; human rights advocates	Practice Internet filtering; take down Web sites; arrest bloggers; and impose other legal restrictions
Equality	Advocates of a New World Information and Communication Order; press and media organizations; developed and developing nations	Efforts to rebalance news coverage; redress inequities; decentralize production of news and information; and diminish the dominance of global media outlets and inequalities in production or consumption
Freedom of Information (FOI)	Civil Society; politicians; NGOs; citizen groups	Develop laws and policies promoting access to government and other public information (eg. encouraging the use of the Web to make information more accessible)
Privacy and Data Protection	Courts; data protection commissioners; law enforcement; government agencies; users and citizens	Enable data sharing; make efforts to protect personal information from unauthorized disclosure; and avoid unwarranted surveillance

Imposing indirect liability on private companies or threatening them with other legal issues has generated fears that industry self-regulation, driven by government policy, will lead to over-zealous censorship online and therefore will decrease or limit access to copyrighted material (Wei 2008). In any case, a narrow governmental focus on law or direct regulation cannot deliver a comprehensive picture of the extent of limitations imposed on freedom of expression online.

Table 4 above illustrates the variety of goals and objectives which underlie explicit or implicit policies of content control within a larger ecology of evolving 'digital rights'.

Censorship: Internet Filtering

The use of filtering software has increased, becoming a common response to controversial online content such as pornography, violence and hate speech. But in some cases, filtering is used for less obviously problematic content if judged as a threat to established norms (Rosenberg 2001). Countries differ in their focus on censoring online material, as well as in their means of blocking content, and in the involvement of citizens in these choices (Bambauer 2008).

Public accountability depends on transparency - knowing what is being filtered, by whom, with what purpose and to what extent. Transparency is one of a number of mechanisms that might enable the public to be more active participants in the decision-making process involved in the use of online filtering systems (Bambauer 2008, McIntyre and Scott 2008). At the same time, as in the case of child abuse images, it is very hard to ensure full transparency where the nature of the content being controlled is such that it cannot legally be accessed, or the website URLs published.

The tension inherent in providing greater transparency and the corresponding benefits of public debate was illustrated by a recent case in the UK. The Internet Watch Foundation (IWF), an independent self-regulatory body tasked with minimizing the availability of potentially criminal Internet content, placed a Wikipedia article on its blacklist, for including an image 'potentially in breach' of the UK Protection of Children Act (Box 6.1).

Box 6.1. Blacklisting of a Wikipedia Image: an Unintended Consequence of Cleanfeed.

On December 5th, 2008, the Internet Watch foundation (IWF) deemed an image from The Scorpions' 1976 album cover 'Virgin Killer', appearing in a Wikipedia article about the album, to be a "potentially illegally indecent image of a child under the age of 18." As a result, the IWF added both the Wikipedia article and the description page of the image to its Internet blacklist. While the legitimacy of this decision has been questioned in its own right, the decision quickly became even more controversial due to the unintended consequences that arose from conflicting interaction between two blocking systems: BT's Cleanfeed technology and Wikipedia's vandalism blacklist.

Cleanfeed is a sophisticated content blocking system designed by BT to block users' access to any pages identified on the IWF blacklist. It is activated on BT retail customers' accounts, and on request to customers of smaller ISPs that resell BT's wholesale service. When a web browser attempts to retrieve a specific web resource, the Cleanfeed system checks the hosting server against a list of IP addresses suspected of hosting pages on the blacklist. If no match is found, the request is completed without interference. However if a match is found, traffic is routed through a small number of proxies that verify the specific page request against the current IWF blacklist. If a match is found the user is met with a standard '404 page not found error', and no information is provided to indicate that the page has been blocked. As a result of this single Wikipedia page being listed on the IWF blacklist, all normal traffic to Wikipedia from ISPs using the Cleanfeed system was rerouted through a small number of proxies.

Wikipedia allows users to anonymously edit most articles on its site, identifying users through their IP addresses. In cases of vandalism or repeated violation of the rules, these IP addresses are blocked. Because BT's Cleanfeed system did not forward the user's original IP address when routing traffic through a proxy server, it became impossible for Wikipedia to uniquely distinguish users. Consequently, the proxy IP addresses were blocked from

Wikipedia and therefore the majority of British users were unable to edit Wikipedia pages.

On December 9th, the IWF rescinded its decision about the blacklisted Wikipedia page, stating that in examining "the contextual issues involved in this specific case and, in light of the length of time the image has existed and its wide availability, the decision has been taken to remove this web page from our list".[37]

Filtering objectives and responsibilities differ across countries. In Australia, for example, a blacklist is generated by the Australian Communications and Media Authority (ACMA). In the future, it is expected to become mandatory for all Internet service providers to comply with the list, although the coverage of that list is currently subject to consultation.[38] In the UK, a blacklist is generated by the Internet Watch Foundation and is made available to all ISPs. The nation's largest ISP, BT, uses this list in conjunction with its Cleanfeed servers to discretely block all URLs from the list (Box 6.1). The National High Tech Crime Centre of the Danish National Police and Save the Children Denmark also generate a blacklist, while in Finland blocking is initially based on a list of Internet domains supplied by the Finnish police.[39] Box 6.2 outlines the situation in Turkey. The European Commission has considered a directive for combating 'the sexual abuse and sexual exploitation of children as well as child pornography', which includes applying mandatory blocking.[40]

Box 6.2. Blocking YouTube and MySpace in Turkey.

In November 2007, Turkey enacted the Turkish Law No. 5651, or the Regulation of Publication on the Internet and Suppression of Crimes committed by means of Such Publication. Since then, thousands of websites have been blocked in Turkey. The exact number is unclear but has been said to range from around 1300 officially 41 to over 6000 websites unofficially.[42] Since May 2008, the Telecommunications Communication Presidency (TIB) has decided to no longer publish any precise statistics related to website blocking based on Law No 5651.This has further reduced transparency in the matter. Some cases of blocking have been court ordered, but most are administrative orders issued by the TIB. Numerous web sites have been blocked because they were considered obscene or including alleged content of child abuse, sexual exploitation, gambling, or prostitution. Other sites have been blocked in Turkey to protect intellectual property. Access to websites such as YouTube, MySpace and the Pirate Bay has been repeatedly blocked ever since Turkish Law No. 5651 was approved, although the block on YouTube was removed on 30th October 2010 and reinstated a month later.

Freedom of Information

The principle of 'freedom of information' was recognized by the United Nations in 1946, under the adopted Resolution 59(1), which stated that:

> Freedom of information is a fundamental human right and…the touchstone of all the freedoms to which the UN is consecrated.[43]

Since then, all three main regional human rights systems (The Organization of American States, the Council of Europe and the African Union) as well as international bodies such as the Inter-American Court of Human Rights and the European Court of Human Rights, have recognized the importance of the right to information, albeit with limitations such as access to any government information (Boxes 2.1 and 6.3). For example, governments would not be expected to divulge much of the information disclosed by WikiLeaks on the wars in Iraq and Afghanistan if deemed to be a risk to individuals or national security (Box 0.3). Nevertheless, principles of the right of freedom of expression include for example maximum disclosure, obligation to publish, promotion of open government, and processes to facilitate access, balanced by considerations such as national security and privacy (Mendel 2008).

There are more than 70 countries around the world that have implemented laws to protect citizens' right to access various kinds of information (Burgman et al. 2008) The Internet has helped many of these countries to provide their citizens access to information related to public bodies, such as parliamentary committees, judicial proceedings, and constitutional decisions as well as related laws and regulations. Indices such as the Index of Online Access to Judicial Information prepared by the Justice Studies Centre of the Americas (CEJA-JSCA) report on the type and amount of judicial information made available online by all countries in North and South America. This leads to greater transparency and accountability on the behalf of governments. When there is a lack of public information online, questions of censorship and filtering arise. In theory, freedom of information and freedom of expression are only limited by a country's laws, especially those related to privacy. But in practice, they are also affected by a much broader ecology of technical, legal and regulatory issues tied to the cultural, political and economic contexts of states (Hamilton 2004).

Box 6.3. International Recognition of the Right to Information

Recognition of the right to information is found in articles pertaining to freedom of expression in international treaties such as the American Convention on Human Rights (Article 13) and the European Convention for the Protection of Human Rights and Fundamental Freedoms (Article 10). More recently, the significance of the right to information was explicitly recognized in other international agreements such as in Article 9 of the African Charter on Human and People's Rights, and further supported with details on how this right should be protected in formal statements made by the African Commission on Human and Peoples' Rights (in the Declaration of Principles on Freedom of Expression in Africa 2002) as well as the Inter-American Commission on Human Rights in the Inter-American Declaration of Principles on Freedom of Expression (2000).
Sources: ECHR (1950), *ACHR (1969),* ACHPR (1981), IACHR (2000), ACHPR (2002), IACHR (2009).

Privacy and Data Protection

Privacy and data protection are driven in part by an interest in supporting the appropriate sharing of data. Advocates of data sharing are right to argue that clarity over the definitions of personal data and the appropriate ways to share these data could help support data sharing regimes. Likewise, uncertainty can put a brake on sharing.

Privacy advocates are increasingly concerned about users' rights to privacy and freedom of expression online, as some see these rights being infringed by government monitoring and surveillance (Brown and Korff 2009). At the same time, citizens and private stakeholders, such as search engine companies, have been the focus of an increasing number of issues over the protection of privacy and data (Tene 2007). For example, individuals with webcams and video cameras are becoming a major instrument for watching other individuals. Instead of the Orwellian Big Brother surveillance of citizens by governments, many see a threat in an equally Orwellian 'Little Sister' surveillance of citizens by other citizens (RAE 2007).

It is difficult to develop a coherent global privacy rights framework with Internet data increasingly flowing around the world and passing through multiple jurisdictions, each with its own data privacy regulations. Conflicting requirements and differing policy definitions and motivations, make the clarification and protection of privacy rights even more difficult (Wafa 2009).

In some respects, privacy is a technical challenge requiring more technologically advanced safeguards to protect personal data that is online. However there are other, more subtle problems in defining personal data on the Internet. For example, the clear delineation of which online content is legitimately public (perhaps a publicly accessible blog post) and what is legitimately private varies over time and across individuals. This is confounded by the development of more refined categories of access. Content is no longer simply private or public, as some information is open to one's family, friends, or anyone else online – the privacy settings on social networking sites such as Facebook allow increasing granularity of control, but with that comes increasing complexity. It is possible that individuals will have a growing number of mechanisms to help them define more precisely the availability of their personal data on the Internet, but this will not solve all problems, so long as some do not understand or use these provisions.

The boundaries between privacy and data protection, on one hand, and freedom of expression on the other, are difficult to establish. This can exacerbate the challenge of protecting freedom of expression online (Erdos 2009). In the EU, attempts have been made to protect freedom of expression within the Data Protection Directive and the Charter of Fundamental Rights.

An example of the potential conflict that could arise from issues on freedom of expression and privacy emerged in a situation involving Google executives in

Italy (Box 6.4). In this case, Google executives were charged with violating the privacy of a child featured in a YouTube video. Holding service providers accountable for all user-generated content that might violate the privacy of an individual, could in turn have a major impact on any large or small user-generated content provider. This case has engendered much debate over Internet freedom and openness, especially in English and Italian speaking media. According to Matt Sucherman (2010), Google VP and Deputy General Counsel for Europe, Middle East and Africa, the Italian court's decision attacked 'the very principles of freedom on which the Internet is built'. Many stressed that the entire Internet was now at risk if "safe harbours" for online service providers were to be threatened in certain jurisdictions (O'Brien 2010).

Box. 6.4. The Google Video Case in Italy

In 2006, a video showing a young autistic person being bullied by his classmates in Turin was posted on Google Video in Italy. The video had been online for a few months before Google was formally notified and then duly took the video down. Nonetheless, after much media attention in Italy, Google was prosecuted for defamation and invasion of privacy. Defamation charges were quickly dropped. However, in February 2010, three of the four accused Google executives were found guilty of invasion of privacy under Section 13 of the Italian Privacy law. Many experts are confident that the ruling will be overturned in Italy, if not in a EU court, where Italian law must comply. Yet, Robertson claims that confusion would still persist in EU courts, as the Google Italy case also discloses flaws in EU law (Robertson 2010). Safe harbour provisions for ISPs, found in the E-commerce Directive in EU law, do not apply to issues related to its Electronic Privacy and Communications Directive. Robertson argues that safe harbour provisions should be completely included or eliminated from both the E-commerce and the Electronic Privacy and Communications Directives (2010). He notes that definitions of 'notice and takedown' in safe harbour provisions are unclear in EU law and requires legislative change at the EU level.

Other experts have argued that the Italy Google case has little to do with freedom of expression, but is rather a concerning case for personal data and privacy issues online (Calo 2010, and Rotenberg 2010). The reasoning for the conviction is apparently grounded on Google Video not fulfilling its notice obligations under Section 13 of the Italian Privacy Code. It was accused of profiting from the presence of ads placed on the Google Video website, by processing personal data it obtained from its users. Yet 'making profit based on relative harm of a person involved' is a violation of Section 167 and not Section 13 of the Italian Privacy Code (Berlingieri 2010)[44].

Ensuring freedom online should not be seen in competition with other goals, such as improving online security and privacy, as in the Chinese case with Google (see section 10 below). Ideally, the broader ecology should be considered in ways that could yield approaches which mutually reinforce a diversity of objectives (Reding 2009). Better solutions or guidelines must be found to balance these Internet rights without undermining fundamental rights.

7. Economic Development and Industrial Strategies

Technology-led Industrial Strategies

Business, industrial and economic development goals have been one of the most significant sets of drivers behind the diffusion of the Internet (Table 5). In developed and rapidly developing countries alike, the Internet is a key infrastructure to support local and international trade and commerce. Financial incentives have led some policy makers to downgrade traditional political risks in order to build not only the physical but also the softer infrastructures of the Internet, such as supporting computer proficiency and skills. However, economic development objectives have not been uniformly viewed as supporting the vitality of the Internet. For example, efforts to protect copyright and patents have led to threats to disconnect users.

Table 5. Industrial Goals, Stakeholders and Strategies in the Ecology

Goals - Games	*Main Stakeholders*	*Strategies - Objectives*
Technology-led industrial strategies	National and regional governments; information and communication industries, firms; users and producers	Develop Internet infrastructures; provide services across all sectors; support take-up by users
Protection of Intellectual Property Rights (IPR): Enforcement of Copyright	Music, film and audio-visual industries; WIPO; national governments; users	Implement digital rights management systems; enforce copyright provisions online; counter Creative Commons initiatives; support bandwidth or speed reduction for offenders; cut off access to major offenders; support deep packet inspection by ISPs
Enforcement of Patents	Software and services developers; national patent offices and agencies	Protection of basic concepts such as 'one-click ordering' or a 'system for exchanging information with friends' that encourages patent trolls; chilling effect on innovation and openness
Competition	Government and industry; business enterprises; producers of computer equipment; related services	Efforts to ensure more competition, less concentration of ownership of infrastructures and content
ICT for Development	Representatives of developing nations, NGOs, Civil Society, ICT	Develop initiatives that foster the diffusion of ICTs in developing nations in

	industries, such as the mobile sector	ways that support production and use, so enabling economic development.

Intellectual Property Rights: Copyright and Patents

The underlying end-to-end architecture of the Internet has made copyright enforcement more difficult. It has supported the creation of open and peer-to-peer (P2P) networks for file sharing. This has led to widespread attempts to strengthen and protect copyrights and intellectual property rights generally.[45] The introduction of a three strikes policy in France (Box 7.1), and the Digital Economy Act in Britain (Box 7.2) are examples of these efforts (Brown 2010).

Box 7.1. The Three Strikes or Graduated Response Law in France.

The graduated response law adopted by the French legislature aimed at enforcing copyright by giving the courts the ability to disconnect Internet users if found guilty of unlawful peer-to-peer file-sharing of copyrighted material. Users who fail to secure their Internet connections, and whose computers are used by individuals other than the owner to unlawfully share copyrighted material, are also subject to penalties. This measure has been contested primarily on due process grounds, as early versions of the legislation did not involve the courts. Later versions have introduced streamlined judicial proceedings to overcome these objections.

Box 7.2. UK Digital Economy Act and Copyright Protection.

In 2009, a Digital Economy Act was introduced in Britain containing a number of measures designed to protect existing creative industries, particularly the music and film industries. It proposed measures that would pressure ISPs to monitor users in order to identify those who are engaging in unlawful file sharing and create the mechanisms to disconnect those users from the Internet. Opponents argued that it was an effort to protect old business models that were not longer viable in the digital economy. Proponents argued that anything else would support unlawful theft of intellectual property. In November 2010 the case for judicial review of the Act was won, and it is expected to come before the courts in February 2011.

The legal protection given to Digital Rights Management (DRM) technology and digital copyrighted material have raised many questions in regards to legal and regulatory issues about intellectual property rights in the digital age. Though numerous European and Asian-Pacific countries have not ratified the World Intellectual Property Organization (WIPO) Internet Treaties and therefore have no obligation to comply with WIPO copyright rules, they still have developed substantial digital copyright provisions (Gasser 2005).

Many point to legislation on intellectual property such as the Digital Millennium Copyright Act (DMCA) as jeopardizing well established fair use rights and the ability to freely exchange scientific research (EFF 2008). There are efforts to redress a balance, led both by pressure groups such as the Pirate Party (Box 7.3) and in some cases by regulators themselves. In Europe, Giuseppe Mazzioti (2008) suggests that Article 10 of the European Commission of Human Rights (ECHR) may be a basis to compel reconsideration of the EU Copyright Law for electronic material. In other parts of the world, such as in developing countries of the Asian Pacific region, revisions of the Trade Related Intellectual Property Acts (TRIPS) agreement and a civil campaign for an Access to Knowledge Treaty have been put forth in efforts to safeguard the public's right to free participation and enjoyment of cultural life and scientific advancement (Wang 2006).

Box 7.3. The Pirate Party.

The formation of the 'Pirate Party' is an innovative political outcome stemming from concerns over Internet regulation. The first Pirate Party was the Swedish Piratpartiet, founded on January 1st, 2006. Inspired by this Swedish initiative, other Pirate Parties have sprung up with growing success in at least 33 countries as of 2009. During the European Parliamentary elections of that same year, the Swedish Pirate Party received 7.13% of the vote. On September 27, 2009, the German Pirate Party received 2.0% in the German federal election.

These party factions cooperate through PP International. According to their Web site, their main interests are:

1. Ending excessive online surveillance, profiling, tracking and monitoring on individuals performed by government and big businesses.
2. Ensuring that all members of society have real freedom of speech and real freedom to enjoy and participate in humanity's shared culture.
3. Reforming copyright and patent laws to legalize non-commercial file sharing and reduce the excessive extent of copyright protection, as well as preventing the use of patents to stifle innovation or manipulate prices.

See: The UK Pirate Party Web site: http://www.pirateparty.org.uk/

In South America, the Argentine Congress has resisted introducing new legislation that would strengthen penalties for criminal violation of intellectual property rights (Aguerre and Mastrini 2009). The Brazilian government has made even stronger moves in taking what they call a first step in protecting user rights and fostering new creativity. In 2009, it presented a draft for a new Copyright Bill that would legalize music mashups as well as copies of copyrighted material for private use (Felitti 2009). Measures such as the Free and Open Source Software Policy (FOSS) were initiated by the South African government in order to lower barriers for adopting ICTs and improve the right and access to knowledge. These are among a number of initiatives

implemented to overcome DRM and copyright provisions which impede access to digital and online material (Schonwetter et al 2009).

ICT for Development

Efforts to diffuse ICTs to developing nations have been primarily led by economic development strategies, as improving Internet infrastructure and expanding access to ICTs are expected to deliver increased prosperity and economic growth. However, the push for Information and Communication Technologies for Development (ICTD or ICT4D) only began to find place on international agendas during the World Summit on the Information Society (WSIS) in Geneva 2003 and Tunis 2005 (Abida 2009). Since then, organizations such as the ITU, UNESCO and the UNDP, as well as the Commission on Science and Technology for Development (CSTD) and the Global Alliance for ICT for Development (GAID) have continued to support discussion of this issue. These groups have helped to sharpen the critical focus on ICT4D, stimulating debate about the financial sustainability of ICT4D projects and also their status in relation to more general issues of Internet governance (Unwin 2009) which has often been mistaken as an issue only for developed nations.

ICT4D focuses on the management of innovative development projects in an effort to support equity and social justice (Gurumurthy 2009). But while mobile penetration rates have more than doubled over the last five years in developing countries, and the Internet has continued to expand globally (see Section 3 of this report), it is estimated that four out of five inhabitants from developing countries still remain offline (ITU 2010). Given this continuing gap, ICTD projects and policies have often been criticized for poor design of information content and weak communication and implementation strategies (Parmer 2009). It is difficult to establish a strong link between the investment in these technologies and the well-being of rural users, or find any evidence of the reduction of information poverty, or any other potential indicators of impact (Casapulla et al., 2001; Keniston, 2002; Ynalvez et al 2010). Furthermore, the multidisciplinary approach to ICTD research has so far failed to properly bridge knowledge and expertise from both the computer and social sciences (Best 2009).

8. Regulating Users: Offline and Online

There is a common perception that the Internet is a ‘Wild West’ or lawless and unregulated territory. This ignores the fact that laws in the offline world also apply to the online world. In fact, user behaviour is very much a focus of law and regulation in every nation, however there are many reasons why criminal behavior is (in practice) less well regulated online. Firstly, many of the simpler regulatory solutions which apply offline (zoning, age restrictions or proof of identity requirements) are harder to implement online. In addition, there is the problem of managing and deploying law enforcement resources online and also the complexity of reconciling cross-national differences in laws and sanctions. Harvard law professor Jonathan Zittrain (2003) argues that

jurisdiction built upon the movement of information traveling across the Internet has proven too costly for governments. However, the extent to which offline laws and regulations targeting user behavior are also applied in the online world can be illustrated by the examples given in Table 6 below.

Table 6. User-Centric Goals, Stakeholders and Strategies in the Ecology

Goals - Games	*Main Stakeholders*	*Strategies - Objectives*
Child Protection	Civil Society; NGOs; governments; parents; police	Take-down of sites; rating and filtering of content; prosecution of offenders
Decency: Pornography	Producers of pornographic films and content; commercial and public service content regulators in nations and regions; the public and consumers	Enabling or blocking production, distribution and consumption of material judged immoral by local standards of decency
Libel: Defamation	Individuals, groups, or firms that are subjects of defamatory claims; the courts; the press and media; bloggers; ISPs	Moving to courts and jurisdictions with lenient libel laws ('libel tourism'); making it easier or more difficult to bring libel actions
Prevention of Hate Speech	Governments; NGOs; civil society; individuals; religious and political groups	Identification of perpetrators, legal restrictions, restricting search, packet inspection
Fraud	Fraudulent sellers and buyers; police; consumers	Efforts to detect and prevent or catch fraudulent sellers and users of the Internet (e.g. phishing)

Child Protection

The Internet is an increasingly central component in the lives of children and young people in the developed world. It cannot be seen as an 'adults-only' environment. It is in this context that some of the most emotive debates around freedom of expression online arise, at the point where the crucial regulatory goal of preventing harm to minors pushes up against the noble ideal of free speech for all. Many, possibly even most states, have introduced some regulatory tools to protect children online, at least in terms of prohibiting illegal activity; the question remains as to how much regulation is enough, and how much is too much. In many jurisdictions, this debate hinges in large part on the distinction between activities that are illegal and those that are harmful.

In attempting to combat activity that is clearly illegal, many countries have expressed revulsion at the production, dissemination, and consumption of child sexual abuse images. In most countries, the removal of these images is deemed to be a justified limitation to freedom of expression. Despite this agreement however, regulatory responses vary, with many countries still

without legislation that specifically addresses child sexual abuse images (ICMEC, 2008). Even within countries with strong domestic legislation that enforces notice and take-down of such material, the challenge of dealing with images hosted on foreign servers is significant. Blocking of such images through the use of blacklists and filters at ISP level is one very obvious response, but one which has its own limitations (see the discussion in Section 4). Should Internet content be controlled by law enforcement agencies or should it rather be a responsibility undertaken by ISPs and search engines? If so, should this occur with or without government support and mandates (Edwards, 2009)? For example, in 2010, the UK's Office of Government Commerce instructed public agencies to only work with Internet service firms that agreed to block websites on the Internet Watch Foundation's (IWF) list of 500-800 child abuse sites (O'Neill 2010). Removal of child abuse images may not be subject to great controversy, but filtering certainly is, even when it remains one of the few tools we have to limit the continuing re-victimisation of those abused.

Once discussion of child protection moves beyond preventing what is clearly illegal towards what is potentially harmful or inappropriate for some users, tensions between rights becomes greater. In countries as diverse as Denmark, South Korea, the United States and Afghanistan, schools and libraries are required to use filtering software to protect children who use their systems. While the ability for consenting adults to opt out of the use of such filters varies between countries, such censorship falls primarily upon disadvantaged people who must use these public facilities to access the Internet (Silenced Report 2003).

Many countries have often used child protection rhetoric to justify laws or regulations that permit filtering or censoring the Internet, such as the Children's Internet Protection Act (CIPA) in the United States, the Clean Feed proposal in Australia and the Green Dam in China (Hull 2008, Maurushat and Watt 2009, OpenNet Initiative 2009).[46] The extent of state responsibilities in protecting children and young people is very much a matter of debate. Some experts argue that regulation may not be the most efficient solution and parents, teachers and childcare workers should be the main reference point to dealing seriously with online child protection issues (Thierer 2007). Others, however, have pointed out that household inequalities are associated with experience of online harm, with the implication that such support networks may not reach all those most at risk from harm (Livingstone & Haddon 2009).

How can the Internet's infrastructure be employed to create an environment where government regulation can be efficient and effective without also being an unreasonable burden (Preston 2007)? The Memorandum of Montevideo promotes a set of standards for Latin American countries and is one example of a regulatory framework that seeks a balance between guaranteed rights for children, and protecting them from online risks. No matter where governments decide to limit freedom of expression rights in the name of child protection, it is important that such regulation be transparent, focuses on specific potential risks, and is measured by its effectiveness. In doing so, governments can employ tools to protect the most vulnerable while lessening risks that their

efforts be perceived as tools of a broader repression of speech (Hills, Powell and Nash, 2010).

Libel for Defamation

Most nations' courts seek to protect the reputations of individuals and companies from irresponsible accusations of libel. However, restrictions on spoken or written expression that are meant to prevent defamation vary widely. In Asia, governments have enacted laws which deter acts of online defamation and frequently impose serious sanctions such as imprisonment. These measures are often seen as stifling freedom of expression and freedom of the press on the Internet.[47] In the US, Australia and UK, libel cases for online defamation have tested the limits of legal jurisdiction in the online world. Britain is widely perceived to have some of the greatest restrictions on the publication of defamatory information, and is said to have spawned libel tourism in the country (Box 8.1).

Box 8.1. Libel Tourism.

As the Internet makes nearly any publication globally accessible, those who feel defamed online can, under the right circumstances, file a lawsuit against a publisher or author in the country where they are is likely to obtain a more favourable ruling. In 2009, the British government planned a reduced cap on the amounts paid to those who successfully sued for defamation, which according to ex Justice Secretary, Jack Straw, was attracting 'liability tourists' to Britain (Mulholland 2009). Mr Straw reportedly said that the abuse of existing libel laws was having a 'chilling effect' on the press by raising the threat of libel suits.

Brenner (2007) has questioned whether online defamation should be subject to prosecution at all, since information flows in an unimpeded way on the Internet. Not only do debates on the limits of legal jurisdiction in the borderless world of the Internet arise, but so do questions on who is ultimately made responsible for online defamation, especially when Internet defamers can remain more easily anonymous and ISPs as well as online content providers are often protected by laws such as the US Communications Decency Act of 1996, which 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 information content provider (47 U.S.C. § 230(c)(1))".[48] The ambiguous definition of service providers was used to avoid censorship by online actors, afraid of being held liable for online defamation. However, this has allowed for the loose interpretation of the law, and in turn means that cases of online defamation involving large Internet companies are usually quickly dismissed. Lone individuals often remain the only ones left needing to defend themselves in online libel cases.

Therefore, liability relating to material online is limited in the fact that:

- Each country can interpret legal jurisdiction according to its own laws.

- Many countries have yet to address issues of online defamation in their legal system.
- New online defamation laws sometimes seem to be a pretext to censor and/or filter freedom of expression and freedom of the press online.
- Ambiguous laws often do not clearly state nor determine the legal liability, role and responsibility of various online actors who could be accused of online defamation (i.e., ISPs, online content providers and producers, bloggers, and journalists).

The ecology of online laws and regulations should indeed assure the right of freedom of expression online as well as individual protection against online defamation. However, it should also hold all stakeholders of the online world responsible for maintaining a healthy and open flow of free information on the Internet.

Hate Speech

As much as the Internet is a mechanism for spreading democracy it is also a breeding ground for hate speech by groups who have used it to promote their cause (Tsesis 2001). While most people tend to agree that this is a negative consequence of the Internet, some think that inappropriate regulation of online hate speech can lead to the suppression of the right to freedom of expression. Others believe that prohibiting hate speech altogether may further proliferate its discourse in society (Cammaerts 2009). Moreover, active censorship usually tends to backfire in a democracy, especially when filtering and online monitoring are used (Timofeeva 2002). So how can a balance be found between both, in order to avoid online censorship (Kakungulu-Mayambala 2008)?

There are two major approaches to this issue. The first is to encourage free and open exchange of ideas online (mainly a US approach). The second is to directly block hate speech on the Internet, which has been the approach adopted by Germany, amongst other countries (Timofeeva 2002). It is difficult and highly unlikely that an international consensus will be found on how to deal with this problem. Some suggest establishing an ombudsman bureau and using exposure as an effective means to reduce hate speech online (Cammaerts 2009). Others argue that the solution lies in public education and the teaching of tolerance and acceptance of diverse values (Timofeeva 2002).

9. Internet-centric Controls and Strategies

Concepts of Internet governance most often evoke discussion of what has been called ‘Internet-centric’ controls and strategies (Dutton and Peltu 2007). These include the regulation of domain names, standard setting, licensing of ISPs, and Internet policies such as ‘Net Neutrality’ (Table 7). We refer to them as *Internet-centric* to bring attention to many other policy areas that also

govern the Internet, such as user-focused policies, and that have been discussed in other parts of this report. Many of these Internet policies have major implications for freedom of expression.

Table 7. Internet-Centric Goals, Stakeholders and Strategies in the Ecology

Goals - Games	*Main Stakeholders*	*Strategies - Objectives*
Domain Names and Numbers	Individuals; firms and organizations using the Web; ICANN; name Registries; the Internet Governance Forum (IGF)	Enable or prevent domain names to protect personal identities, businesses or online traffic, such as new top-level domains, (eg. dotXXX)
Internet and Web Standards: Identity	W3C; IGF; national and regional Governments	Create standards that prevent or protect the anonymity of users
Net Neutrality	National telecommunication regulators; the Internet Industry; advocates of end-to-end Networks	Using regulation to protect end-to-end principles of service provisions over the Internet
Licensing and Regulation of Internet Service Providers	ISPs; national governments and regulators; ICANN; users and content providers.	Keep ISPs close to, or at arms length from, governmental or commercial pressures, to control their independence

Internet Governance and Regulation

Information Infrastructure is an initiative started by the US government in 1993 as a new telecommunication policy for the Information Age. Since then, numerous international forums, summits and meetings have taken place in efforts to find an effective way to regulate the Internet (Berleur 2008). From self-regulation to government intervention, the Internet community has suggested a variety of different approaches to regulation, but many believe they have failed to govern it effectively (Kesan and Gallo 2006).

The Internet Corporation of Assigned Domain Names and Numbers (ICANN) has played a fundamental role in shaping the technical infrastructure of the Internet and has subsequently taken on much responsibility for its governance in some fairly specific areas. However, there are many who question the legitimacy of ICANN's role (von Bernstorff 2003) and others who refute numerous ideas that associated Internet governance with ICANN (April 2006). The influence of ICANN specifically, and the 'West' in general, have been an enduring issue in the World Summit on the Information Society (WSIS) and the IGF.

The Working Group on Internet Governance (WGIG), which was established as a follow-on from WSIS, defined Internet governance around a multi-stakeholder approach to developing 'shared principles, norms, rules, decision-

making procedures, and programmes that shape the evolution and use of the Internet' (WGIG 2005: 4).

The Internet's architecture has never been an object of national regulation and has remained open to international consensus. ICANN has been responsible for the management of IP address space allocation, protocol identifier assignment, top-level domain name system management, and root server system management functions. This organization refers the associated technical work to IANA or the W3C, which function as the international standards organizations for the Internet. ICANN, the Internet Assigned Numbers Association (IANA), and the W3C operate at an international level to introduce Internet-wide principles. The challenges facing Internet governance are in part due to the uncertain legitimacy of existing bodies, such as ICANN, and the degree to which these institutions focus on only one of many areas of policy and regulation shaping the future of the Internet.

However, these actors have established a set of principles to guide their work - openness, interoperability and neutrality – which have gained legitimacy in debates over many areas of Internet regulation and governance (Dutton and Peltu 2007). This can, if permitted, support an environment where users can express themselves freely without fearing control or censorship by monitoring bodies. The neutral character of the Internet is a key element in maintaining a free and open approach to Internet-based communication, speech and expression. Thus, the Internet as an infrastructure, which enables an almost real-time upload of recordings and documents, has become an object of international policy.

Specific technical matters can have an influence on policy-making and present implications on freedom of expression and the openness of the Internet. Matters related to Internet address space (e.g. the transition from Internet Protocol Version 4 (IPv4) to IPv6, the scarce resource of IP addresses, address hijacking and the sometimes unstable change of protocols) or the Domain Name System is by nature regulating the Internet and access to it. Limitations to American Standard Code for Information Interchange (ASCII) or the exclusion of non-Latin letters in using top-level-domains can be seen as a constraint to freedom of expression. Innovations aimed at addressing these limitations are currently being developed (Box 9.1).

Box 9.1. Emergence of Internationalized Top Level Domain Names (IDNs).

ICANN has introduced internationalized country-code top-level domain names, which will enable the introduction of a limited number of IDNs for country code top-level domains (ccTLDs). Thus, it will be the first time that users can obtain a domain name with the entire string in characters based on their native language. The process will be available to all countries and territories where the official language is based on scripts other than the Latin (extended) script. The first non-Latin top-level domains were added to the DNS root zone in May 2010.

See: http://icann.org/en/topics/idn/

Regulatory Models for a 'Technology of Freedom'

Many scholars have viewed new media as inherently free – the so-called 'technologies of freedom' (Pool 1983) – given the shift from:

- only a few to a burgeoning number of content producers;
- local and national systems to global networks;
- real time to asynchronous communication; and
- control of access and content shifting into the hands of users, who are also producers.

Finding an appropriate regulatory model for the Internet has been difficult. In the past and still today, old models do not apply. Yet the search for a new model was not a priority before, given that it was not regarded as a serious threat to existing broadcasting and print media, as well as to telecommunications. The dot-com bubble that sank many new Internet companies between 1998 and 2000 vindicated this position for many.

However, the growing diffusion of the Internet since 2000 has led to the Internet being viewed as the future of information and communication technologies. It is perceived as a technology that has disrupted traditional media and their business models in ways that threaten their business strategies and the regulatory regimes that govern them. This new position in which the Internet finds itself leads to initiatives aimed at Internet governance and regulation, such as in establishment of the Internet Governance Forum (Box 9.2), which is a set of factors in the ecology of freedom of expression. Notwithstanding these recent developments, access to the Internet has been the major engine behind this technology of freedom, and the freedom of connection.

Box 9.2. The Internet Governance Forum (IGF).

The IGF was one of the most tangible and significant outcomes of the World Summits on the Information Society (WSIS) in 2003 and 2005, organized by the UN and International Telecommunication Union (ITU). The WSIS pioneered a new kind of global politics in which the role of civil society has become more formally acknowledged within a multi-stakeholder approach to policy, broadening governance beyond the domain of governments to include business, non-State, and civil society actors in a form of multilateralism.

The Working Group on Internet Governance (WGIG) was set up after the first WSIS phase in Geneva, to explore the roles and responsibilities of Internet governance stakeholders and to identify key issues for both developing and developed countries. The IGF was formed after the second Summit in Tunis, as specified in the WSIS (2005) 'Tunis Agenda for the Information Society' that took account of recommendations by the WGIG (2005). The IGF inherited values favouring: a multi-stakeholder approach; a broad view of the social,

economic and cultural impacts of the Internet compared to a previously narrow focus on technical issues through bodies such as the influential Internet Corporation for Assigned Names and Numbers (ICANN); and an emphasis on the link between Internet governance and development strategies to meet the goals of the UN's Millennium Development Goals. Since the formation of the IGF, many nations have sought to develop national IGFs to develop more consensus and organization at the national level.

Protective Regulation: Net Neutrality

Net neutrality is one of the more technical aspects of Internet regulation that has been viewed as a potential threat to freedom of expression online. There is no single definition for net neutrality but it usually means that ISPs do not discriminate against users through access fees, nor do they favour one type of content or content provider over another, or charge content providers for sending information to consumers over their broadband cables (Hogendorn 2007). As digital media evolves with the creation of new technology, the need for bandwidth has made the net neutrality debate more prominent (Bailey 2008). It is attractive to many as a possible solution to managing existing bandwidth more efficiently as demands begin to exceed supply, rather than simply expanding available bandwidth.

Net neutrality has often been viewed as a North American issue, though regulatory policy in Europe and elsewhere would indicate otherwise (Marsden 2009). The Internet is increasingly being threatened by privatization (Nunziato 2008) and net neutrality has become linked with approaches to vertical integration between content and conduit (Wu and Yoo 2007). This has many people worried that ISPs will incur discriminatory actions and online content will therefore not be accessible to everyone in the same way, possibly creating a two- or multi-tiered Internet.

Some ISPs have already employed discriminatory practices such as throttling, to ensure that high bandwidth users do not slow down overall Internet traffic. This has distanced them from concepts of net neutrality, albeit in the interests of improving service. Part of the debate is determining what is good and bad discrimination (Wu and Yoo 2007) and what kind of policy or set of laws should governments adopt in order to ensure fair access to broadband Internet? Cheng et al. (2007) have argued that net neutrality regulation will incentivize ISPs to invest in broadband infrastructure at a more socially optimal level. Often ISPs under- or over-invest in infrastructure capacity when there is a lack of regulation (ibid). Atkinson and Weiser (2006) recommend that policymakers promote more market entries by new broadband providers and adopt policies that boost the size of 'best-efforts' broadband connections. In contrast, Marsden (2007) suggests a 'light-touch regulatory regime involving reporting requirements and co-regulation, with as far as it is possible, market-based solutions'.

Licensing and Regulation of Internet Service Providers

ICANN has been the key institution delegating various rights and responsibilities to organizations for the assignment of domain names and numbers around the world. This provides the basis of a growing industry of Internet domain name registries, similar to Nominet UK, or Afilias. Additionally, a growing array of business enterprises such as Google or Yahoo! are licensed within countries to provide an array of Internet services, ranging from defence to search. The licensing of businesses and the allocation of responsibilities are becoming some of the key elements of the ecology of Internet freedom, as governments can intervene in various ways to pressure businesses to conform to national law and policy. The threat of licence loss is a mechanism that an increasing number of countries use to transfer regulatory burdens, such as monitoring Internet use, to service providers, as proposed by the UK's Digital Economy Act (Box 7.2.)

10. Security

Security concerns are perhaps the primary motivation of many governments in seeking to gain better control of the Internet. These include the desire to identify Internet users, protect consumers from spam, reduce criminal activities and stop national security breaches. The area has been the subject of extensive discussion and this section will only seek to illustrate the many ways in which the goals and objectives of stakeholders in the security realm can be understood within conceptions of the larger ecology of expression (Table 8).

Table 8. Security Goals, Stakeholders and Strategies in the Ecology

Goals - Games	*Main Stakeholders*	*Strategies - Objectives*
Secrecy, Confidentiality	Government; diplomats; parliamentarians; the press; bloggers and information providers	Super-injunctions to prevent news coverage of parliamentary proceedings; intranets and firewalls to prevent public access to corporate or public information deemed confidential
Security against malware, such as spam and viruses that disable computers	Virus writers; users; Internet equipment and service providers; government and law enforcement	Creation of identity systems and software to detect and remove viruses; efforts to track and charge producers of malware
Counter-Radicalisation	Political, religious groups and individuals; law enforcement; foreign affairs agencies; community leaders; parents	Efforts to discover individuals and contexts subject to radical ideas; open dialogue; promote exposure to countervailing information and ideas
National Security,	Law enforcement; national	Efforts to prevent or detect

Counter-Terrorism	security agencies; ISPs; Internet users; business and travel firms and services	efforts to breach security of computers, locations, or services

Governments worldwide are seeking to balance online freedom of expression with many other objectives. National security is a critical goal for most in an ecology that ties national security interests to those of advocates of freedom of expression. Foreign diplomacy requires confidentiality, and exposure can cause great embarrassment, as illustrated by the release of diplomatic correspondence by WikiLeaks in 2010. Companies seeking to do global online business find themselves forced to understand how to comply with local and national laws, regulations, and customs that vary across jurisdictions. In doing so, defending, sacrificing or adapting principles related to freedom of expression are one aspect of business decisions with multiple legal, commercial, and ethical concerns.

Two recent cases have highlighted the ecology of games that is shaping the strategies of nation states and some of the Internet's largest commercial interests: Google in China, and Blackberry in the Middle East.

Google and China

In 2010, Google has continued to be the world's most popular Internet search company, maintaining offices in dozens of countries and offering search results in over 100 languages. The corporation has been clear on issues of freedom of expression: Google's stated mission is 'to organize the world's information and make it universally accessible and useful'.[49] Nevertheless, Google faces requests to remove or restrict information from many countries, including Brazil, Germany, India and the US, and seeks to comply fully or partially.[50] From time to time, Google's decisions have stirred controversy. The most notable example of this, and one that illustrates the ecology of games in freedom of expression online, involved Google's relationship with China.

Until 2006, Google had no headquarters with employees in China. However, it provided a Chinese language version of Google.com that was easily accessible to users in China. In 2002, China began blocking access within the country to Google's servers. As Google explained in its testimony to the US House of Representatives Committee on International Relations:

> [Google] faced a choice at that point: hold fast to our commitment to free speech (and risk a long-term cut-off from our Chinese users), or compromise our principles by entering the Chinese market directly and subjecting ourselves to Chinese laws and regulations. We stood by our principles, which turned out to be a good choice, as access to Google.com was largely restored within about two weeks.[51]

However, Google faced more problems over the next three years when access was sporadically blocked or slowed. It became clear that the Chinese

government was filtering search results. Google users found requests were often denied or redirected to other search engines operating within China and were subject to strict censorship requirements.

Facing such difficulties, and losing market share to their major competitor, Baidu, Google decided in early 2006 to reverse their stance against self-censorship. They opened offices in China and began operating Google.cn. In doing so, they committed to respecting the content restrictions imposed by Chinese law and regulations, as they do in other countries in which they operated. Google argued that their decision that censored access was better than no access at all, yet many accused Google of putting their business interests ahead of their commitment to freedom of expression.

Google continued to auto-censor results on Google.cn until January of 2010 when the search engine announced that the company, along with at least 20 other large corporations, had faced sophisticated cyber-attacks originating from within China (Box 10.1). These attacks lead to the theft of intellectual property for Google and the unauthorized access to the email of dozens of human rights activists. Consequently, Google announced that it would stop censoring its search results on Google.cn and operate an unfiltered search engine, even if this meant closing its offices in China.[52]

Box 10.1. Google and China, 2010.

On January 12th, 2010, Google announced that it would stop censoring its Chinese search engine, Google.cn, after claiming to be victim of a targeted attack originating in China. Google cited that the goal of the attackers was to access Gmail accounts of Chinese human right activists. This was not the first incident in which commercial Internet firms were believed to have been targeted. In 2005, Amnesty International claimed that the Chinese government had employed user email account information provided by Yahoo to sentence Chinese journalist, Shi Tao, to 10 years in prison. However, at the time of publishing, only two Gmail accounts appear to have been accessed and limited information (such as subject lines, time and date) rather than actual email content were retrieved. The search engine also declared that dozens of Gmail users based outside of China, who were human right activists, had their accounts routinely accessed by third parties - likely by phishing scams or malware placed on the users' computers (Drummond 2010).

Google originally launched the Chinese version of its search engine in 2006 and had agreed to censor certain search results, such as the Tibetan independence movement, the Falun Gong and the Tiananmen Square protests of 1989, in order to comply with government terms and rules. The search engine had been criticized by human rights and Internet advocates for adhering to China's restrictions on freedom of expression. Google argued at the time that, even though filtering 'severely compromised' its mission, not providing any information at all to a fifth of the world's population was far more severe (McLaughlin 2006).

Even if Google.cn had been filtering to comply with Chinese regulations, up until this recent announcement Google.com had not been subjected to the same type of censorship as other Chinese search engines and websites and was fairly accessible to Chinese users (Canaves 2010).[53] Although Google is using human rights issues as a rationale to stop filtering search results in China, there were speculations about underlying motives for this announcement. Some have argued that this unprecedented decision was a move by Google to improve its reputation in the West, especially amongst the European community where concerns over privacy issues are growing (Morozov 2010).[54]

Reaction to Google's announcement was mixed. The US Congress announced an investigation into the cyber-attacks. US Secretary of State, Hillary Clinton presented a well-publicized speech about Internet freedom and made reference to Google's announcement by requesting transparency from the Chinese government and highlighted that the United States and China had "different views" on the freedom of information online.[55]

The Chinese media responded by accusing Google and the US government of trying to use the Internet to impose Western values worldwide. Links between Google's commercial decision and the politics of freedom of expression were boldly presented by China's People's Daily Online as a move that politicised a commercial decision.[56]

In March 2010, Google stopped censoring its search service. From then, users visiting Google.cn were redirected to Google.com.hk, where Google offers uncensored search results delivered via servers housed in Hong Kong in simplified Chinese. As China's content restrictions do not apply to services in Hong Kong, Google felt that this solution was consistent with Chinese law. China appeared to accept this remedy.

Google's announcement highlighted some of the other players in this ecology of games. For example, while moving its search services, Google announced its intention to continue Research & Development work in China and also maintain a sales presence in the country.[57] In doing so, Google is drawing a link between their contribution to the Chinese economy as an employer and their ability to operate with minimal restriction, thereby adding their employees to the ecology of games. The role of Google's employees in this ecology is also highlighted by Google's statement that 'these decisions have been driven and implemented by our executives in the United States, and that none of our employees in China can, or should, be held responsible for them'.[58]

Privacy versus National Security: Blackberry

Canadian company Research in Motion (RIM), the makers of the Blackberry, has faced pressures from governments around the world to allow access to information sent and received from their popular Blackberry devices. Government representatives in the United Arab Emirates, Saudi Arabia, Indonesia, India, and Bahrain have argued that RIM's encryption of Blackberry messages posed national security threats and that the routing of

data to RIM's offshore servers put control over data beyond the scope of national regulators and law enforcement. Saudi Arabia and the United Arab Emirates have threatened a shut down of Blackbery services within their respective national borders if RIM could not find a technical solution that would enable security services to monitor Blackberry communications.

The pressure on RIM in their decisions to allow monitoring of communication is complicated by several factors. A major selling point of the Blackberry has been its encryption, which is designed to make its messenger service more difficult for anyone, including RIM, to monitor. Market pressures, however, seem to be pushing RIM towards technical monitoring, with stock shares falling as governments have threatened shut-downs, and rising on news of technical solutions for monitoring.[59] RIM is also dependent on service providers in other nations to provide cellular access for their Blackberry devices. In cases where service providers are more tightly controlled by government agencies, governmental pressures on these providers can put them at odds with RIM.

Pressure to provide government access to cryptography keys is not a recent development, nor is it isolated to the regions currently placing pressure on RIM. Proponents of strong cryptography point out that such access is fundamentally flawed because of its dependence on key escrow. Key escrow involves providing a third party with the keys to decrypt encrypted information so that the third party can access the information when necessary, such as over concerns related to national security. However, by introducing a third party into the encryption relationship, the protection of the cryptography becomes a greater social and political, rather than technological, challenge.

Processes, regulations, laws, and reviews must be put in place, followed, and trusted, in order for the security of the information to remain intact. Key escrow systems have traditionally met with stiff resistance and technological failure, such as attempts to introduce the Clipper Chip (Box 10.2).

Box 10.2. The Clipper Chip.

The Clipper Chip initiative was launched by the US government in 1993. This would provide chips that encrypted communications with a secret algorithm developed by the National Security Administration. As part of the initiative, all Clipper chips contained a cryptographic key that was also provided to the US government under a key escrow system. This enabled greater privacy of communication for individuals, balanced by processes for protecting national security. Critics claimed that the system opened citizens to the possibility of unauthorized government surveillance. While the US government initially stated that the use of the Clipper chip would be voluntary, critics saw its introduction as the first step toward outlawing other forms of cryptography, which has been a concern of national security agencies.[60] However, controversy over the chip, and the development of effective public alternatives, eventually derailed the Clipper chip initiative, leading the US government to stop pressing for its adoption.

Secrecy and Confidentiality

In direct contrast to freedom of information concerns, there remain areas of public processes that are judged by many to be better served by maintaining secrecy, or confidentiality. For example, the confidentiality of jury deliberations is protected. In such cases, openness might jeopardize the fairness or justice of a proceeding. Like privacy, the need for secrecy or confidentiality, if justified, can counter freedom of information as argued in opposition to WikiLeaks' distribution of confidential information (Box 0.3). In cases where data is confidential or sensitive, security breaches can be a major threat that needs to be balanced with countervailing calls for sharing or providing government data. As discussed below, this is one of many motivations behind efforts to better identify users, such as in cases when it would be possible to identify the individual that posted or emailed information that was to be kept confidential.

Security against Malware

Individual users concerned about malware, such as spam or viruses, normally want to filter spammers and malicious hackers seeking to install viruses on their computer. They also might want better information about who is emailing them, or asking them to establish a connection within a social networking site. This is another motivation for identifying the person sending a defence or requesting a link: Is the requester who he or she says they are? Some people want to know to whom they are speaking in certain situations. However, there are solutions to identifying 'badware' by obtaining information, for example, about requests that ask users to install software on their computer (Box 10.3).

Box 10.3. StopBadware.

One project, called StopBadware, seeks to use many web techniques to monitor those who might distribute malicious software. If a user is asked to download a program on their computer, for example, StopBadware would inform the user about the software, such as how long it has been in use, and how many computers have installed it. A very new piece of software that is installed on few computers would be a higher risk, enabling users to make a more informed decision without knowing the exact identity of the provider. The project seeks to provide other services, such as a clearing house function, as a place to report suspicious or bad software or services.

Source: http://stopbadware.org/

Increasingly, good and bad actors online have an interest in monitoring the use of the Internet to identify malware providers or to be aware of spammers. Assuming that actions are monitored and that online behavior is traced and tracked, user communities can keep people from accessing or posting particular content. In many countries monitoring is permitted in controlled circumstances by law enforcement and intelligence agencies through a variety of methods (Box 10.4).

Box 10.4. Methods of Monitoring Internet and Web Traffic.

- Intercepting communication transmission via a telecommunications system (such as a computer) and divulging information to a third party on account of national security, the prevention or detention of serious crime, or the economic safeguarding of a state.[61]
- Logging, recording, retaining, and giving access to information about visited websites, emails sent and received, or applications used.[62]

Source: Brown (2008).

National Security: Counter-Radicalization and Terrorism

Internet use in terrorist activities, ranging from efforts to radicalize youth to managing radical interests, has created the most recent and serious motivation behind efforts to monitor the Internet and identify users (Box 10.5). The actions required to better survey speech online and distinguish who says what, to whom, are not in themselves a threat to most users of the Internet. They nevertheless can have a chilling effect on the completely legitimate use of Internet.

Box 10.5. Online Identities: Part of a Bigger Picture

The issues surrounding identities online are complex and critically important, yet they need to be addressed in relation to the larger ecology of issues in which they are embedded. Changes in the ways identity is handled on the Internet can have unintended consequences, such as jeopardizing the Internet's value as a new space for democratic expression and accountability. Inevitably, a number of working groups and conferences have been organized to address these issues.[63] The problem is that no single level or standard of identity is appropriate for all activities. For example, freedom of expression often requires anonymity, yet many other activities and services have need for user identification. While not everyone agrees in creating what some have called the 'accountability versus anonymity' debate, it is an important issue to address.[64] Often there is only a need to authenticate that a person has a right to the service, such as being over a certain age. Therefore online identity systems must support this broad range and not require a level of identification greater than required by a particular service. One European advisory board on identification made the following recommendation:

> 'The EC, together with the Member States and industrial stakeholders, must give high priority to the development of a common EU framework for identity and authentication management that ensures compliance with the legal framework on personal data protection and privacy and allows for the full spectrum of activities from public administration or banking with strong authentication when required, through to simple web activities carried out in anonymity ' (RISEPTIS 2009: 31).

Some within the technical community might want a one-size-fits-all system for

identifying users because it is easier to design and implement. However, in real life there are many different levels of authentication and identification required, depending on the circumstances. Online, the idea of one technically driven standard would be problematic.

11. Summary and Conclusion

The Ecology Shaping Freedom of Expression

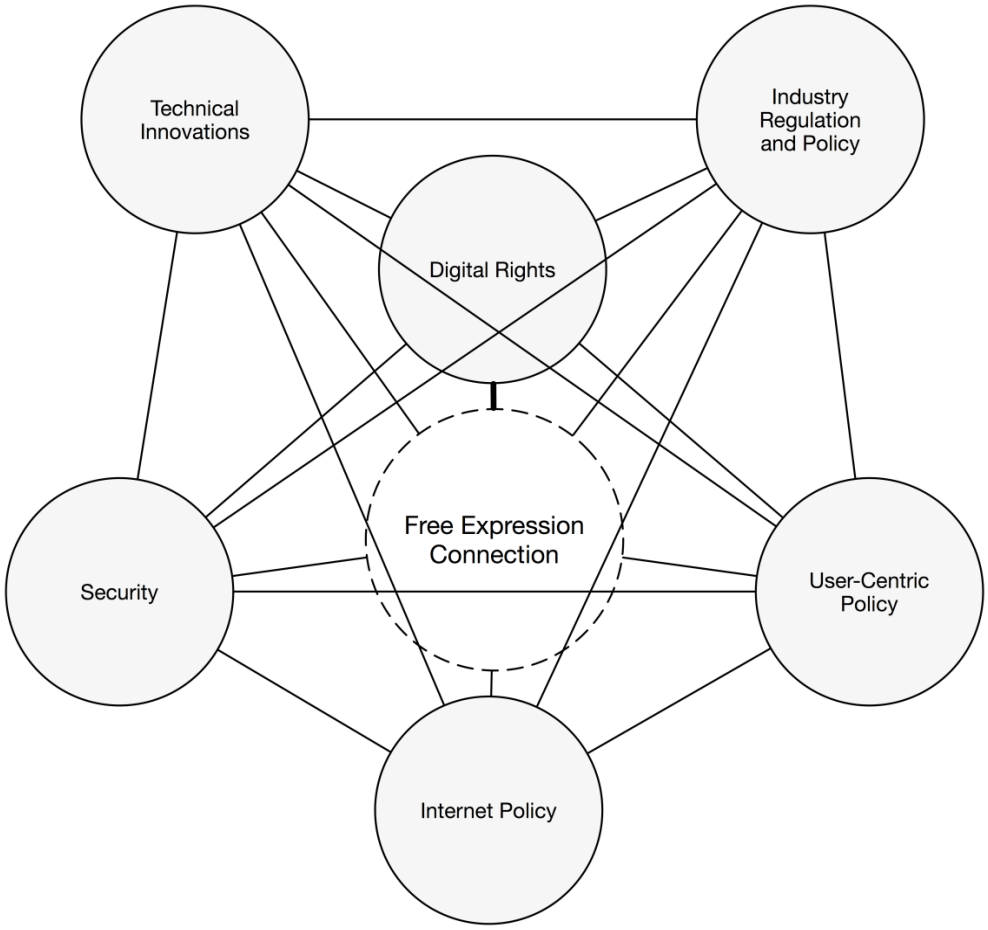
Internet stakeholders ranging from government and regulatory bodies to ISPs and civil society advocates, are increasingly addressing issues tied to freedom of expression online. This report has highlighted the multiplicity of policy issues shaping online freedom of expression around the world. For example, the control of spam and viruses is one well-accepted rationale for Internet service providers to justify the monitoring of online traffic in order to protect users. However, many other areas such as libel, defamation and intellectual property protection, are providing reasons for greater control of online content in ways that fundamentally affect multiple actors, ranging from users, webmasters and bloggers to ISPs. They also have more general repercussions for those prosecuted under these laws in ways that can disproportionately constrain freedom of expression.

Censorship of the Internet, as evidenced by national filtering of online content, appears to be more widely acceptable, even within states with liberal democratic traditions. Concerns over issues such as child protection, online decency and fraud have been deemed significant enough to justify restrictions on freedom of expression. This is not to say that such considerations are not important to address in the digital age; the eradication of child abuse images online, for example, is almost universally accepted as a vital goal. Yet our research indicates that disproportionate reliance on disconnecting users or filtering content could seriously undermine essential aspects of freedom of expression without resolving the policy problem at hand, unless the larger ecology of policies and regulations are taken into account in balancing conflicting objectives. Protecting certain human rights or freedoms often has a direct and immediate impact on other rights and freedoms. Thus, the preservation of one freedom can limit another. Balancing these conflicting values and interests is only likely to be a resolved through negotiation and legal-regulatory analyses. This will probably vary cross-nationally, if not locally. Resolution of these balancing issues requires a broad view of the larger ecology of policies and regulations shaping freedom of expression (Figure 9).

Freedom of expression and the right to communicate are, in many ways, being redefined by the development of and access to new technologies. Modern progress on the Internet challenges, yet also enables, freedom of expression. Today we see the emergence of two types of filtering variously applied in different nations and regions of the world: 1) filtering for the

protection of other citizen values, such as privacy or child protection; and 2) filtering to impose a particular political or moral regime, such as entailed in governmental surveillance or political repression. In essence, while these intentions are not always explicit or distinguishable, they suggest room to move to a more instrumental acceptance of online content controls, based on the motivations underlying the activity. This in itself is a potentially major shift from a more blanket rejection of censorship in the era of the mass media and the early years of the Internet.

Figure 9. The Ecology of Freedom of Connection and Expression



It is critical that more international bodies and scholars be concerned with these topics. The benefits of open, free expression, and freedom of connection are immense. There are many ways to mitigate the risks of an open society and filtering or censorship are rarely the most effective of these. This report has introduced a new and broader conceptual framework for discussing the legal and regulatory trends that are shaping online freedom of expression around the world – when fundamental freedoms are increasingly tied to the Internet. It is our hope that such a conceptual framework will focus more attention on: 1) identifying and clarifying the diversity of associated actors, goals and strategies that affect freedom of expression and connection; 2) facilitating more comprehensive and coherent discussion and debate on

the ecology of legal and regulatory choices affecting freedom of expression on the Internet; and 3) establishing areas in which empirical research could inform debates over policy and practice.

Recommendations for Research, Policy and Practice

This review and synthesis of previous research and related literature provides a basis for recommendations related to research, policy and practice. UNESCO and its constituencies should consider the following:

Continue Efforts to Support the World Wide Diffusion of the Internet

One of the most positive developments in supporting freedom of expression has been the role of the Internet in enabling greater worldwide access to information. The Internet and Web have allowed individuals to network locally, nationally, and internationally in ways that can create new forms of democratic accountability (Dutton 2009). Many nations have not yet achieved high levels of adoption, such as in Asia, but have nonetheless seen the migration of a large number of individuals to the online world. The growing numbers of people online make the Internet an important information and communication resource in these countries.

Nevertheless, continued efforts to support the development of the Internet through new infrastructure, such as the deployment of undersea fibre optic cables in East Africa, or the increase of multi-media awareness and proficiency in schools, should be nurtured. In his first speech after resigning as Prime Minister of Britain, Gordon Brown spoke from the capital of Uganda, saying: "… I truly believe that the rapid expansion of [I]nternet access in Africa could transform how Africa trades, learns and holds political power accountable."[65] This vision requires worldwide attention to balancing the conflicting values surrounding access in ways that protect freedom of expression and connection.

Other endeavors, which support the growth of a multilingual Internet, such as the development and translation of relevant content in local languages, can also foster the sharing of ideas and dialogue across nations, helping to support freedom of expression online. If everyone is to enjoy the right to freedom of expression, it is important that the Internet's ability to advance free and open speech is recognized and that measures are taken to make the Internet as accessible as possible to all.

Recognize the Internet as a New Arena for the Defence of Democratic Values

The Internet is becoming more central across the world for shaping access to treasures of information and expertise, but at the risk of endangering values like privacy, personal reputations, and freedom of expression. Debate over fundamental human values will increasingly focus on the Internet as much as on traditional media and face-to-face modes of communication. This is not a temporary phenomenon, but the beginning of recognizing that communication

will be increasingly reliant upon an online platform at all levels for numerous media, from the hyper-local to the global.

Renew and Inform Debate over Appropriate Regulatory Models

Despite common appeals to freedom of expression around the world, there is continuing uncertainty over what constitutes the most appropriate regulatory model to govern information networks and related ICTs. This has been an ongoing debate since the 1970s, when visions of the future of computing began to undermine old paradigms of mass media. The Internet's distinct structure has raised many questions and challenges for existing regulatory models, designed for common carriers and traditional media. As the Internet has become more global with satellite communication and trans-continental fibre networks, and more central and increasingly inseparable to the media landscape, the application of old regulatory frameworks to the Internet seems to have continued without sufficient discussion of its likely implications. Moreover, the regulation of this distributed 'network of networks' has been made increasingly feasible through the development of tools and strategies for filtering and censorship.

The question therefore remains: Should the Internet be regulated as if it were a newspaper, broadcaster, or a common carrier network? Or should it follow a new regulatory framework, which could well be the most sensible way forward (de Sola Pool 1983; Dutton 1999; Vries 2005)? Some have viewed content on the Internet as impossible or inappropriate to regulate, a position well developed and most influenced by Ithiel de Sola Pool (1983) in his discussion on videotext. Impossible, because control over content production and consumption on the Internet was thought to be inherently distributed and incapable of being centrally controlled or censored. Inappropriate, because computers were thought to become newspapers of the future and should therefore enjoy the same freedom as the press.

In line with this thesis, many Americans now argue that a strict interpretation of the US First Amendment should be extended to the Internet. American courts have supported this view, arguing that factors such as a broadcaster's pervasive nature, which justified broadcast regulation, were 'not present in cyberspace' (US Supreme Court 1997). On the basis of these rationales, many nations, even those without policies or traditions in line with the First Amendment, have limited governmental regulation of the Internet, making it one of the most open media for free expression. Further discussions and informed debate are needed to develop a suitable regulatory model for the Internet to ensure the protection and advancement of an open and free culture online (Steven 2000, Balkin 2004).

Strengthen and Clarify International Mechanisms for Internet Governance

Many factors confront a global network, such as the Internet, that are not as critical to older national and local networks. For example, uncertainty over questions of governance and regulation as well as cross-border issues, have made it particularly difficult to effectively protect freedom of speech in the

information society (Graux 2009). New technologies make information and cultural production valuable commodities in a global market in ways that could create restrictions on freedom of expression (Balkin 2008). In particular, the protection of copyright can place new constraints on freedom of expression as discussed earlier in this report. In other instances, controversy over the jurisdictional authority of existing Internet governing bodies, such as ICANN, have led to nations asserting more sovereign claims in areas of domain registration and in Internet governance generally. Furthermore, international variations in governing norms on free expression online have prevented ICANN and the IGF from taking stronger positions to protecting freedom of expression on the Internet (Nunziato 2003).

The rise of national Internet governance and regulatory initiatives could be a response to the failure of international institutions to play a more effective role. However, the Internet is not limited by political boundaries and national governance could therefore create disjointedness on the Internet, possibly undermining its free and open nature that helped create the vitality behind its worldwide diffusion. This is why there is a need for a stronger multi-stakeholder framework for Internet governance at the international level. Freedom of expression stakeholders should be particularly involved in the Internet governance process in order to preserve the right to free speech and connectivity online. The creation of a special international taskforce for freedom of expression should thus be considered in order to support and represent these stakeholders in Internet governance.

Better Monitor World Wide Internet Filtering

The OpenNet Initiative and other research groups have conducted groundbreaking research, which focuses on monitoring the filtering and blocking of websites overtime and across jurisdictions. However, many countries have not yet been studied, and the sustainability of this research is unclear, particularly if expanded to a larger proportion of countries. More resources should be devoted to the global monitoring of Internet filtering and censorship. This is a necessary condition to have more informed debate over the practice and impact of filtering technologies and policies.

Understand Shifting Public Attitudes and Expectations

Many factors are shaping the experience of individuals and nations with respect to freedom of expression and connection. People are sensing greater freedom of expression, even in nations with aggressive filtering practices. This is possibly due to the Internet opening up a new channel for communication. Technical and historical outcomes from the Internet will be experienced at the individual level around the world. Therefore, more research needs to be done to tap into cross-national and longitudinal comparisons of attitudes, beliefs and actions about freedom of expression. Do people believe that they have more or less freedom of expression online? What is the basis of their attitudes and beliefs? What does freedom of expression actually mean to them? The World Internet Policy Project (WIP2) has already presented work along these lines and the topic has recently been broached in a 2010 BBC global survey.

These empirical efforts should be critically assessed and refined in such ways that these efforts can be continued and supported.

Monitor and Document the Diffusion of Legal and Regulatory Initiatives

Work is needed to monitor and document more systematically the legal challenges that test freedom of expression online in various jurisdictions, as well as the legal and regulatory initiatives that are creating these issues. This will help to identify the barriers people face in freely expressing their opinions online and how legal and regulatory frameworks should be shaped in order to encourage a free and open Internet. The scope of this effort should be as broad as the wide ecology of freedom of expression sketched in this report.

Cultivate Citizen Consultation and Decision-Making

All actors involved in the control of content in the digital age should explore how citizens can more actively participate in the decision-making processes tied to the use and misuse of filtering systems online (as noted by Bambauer 2008, McIntyre and Scott 2008). User-generated content processes can be employed to provide feedback on inappropriate material but also on questionable filtering practices. For example, panic buttons on some sites permit children to report situations in which they are frightened by an interaction online. Should people be able to report situations in which they believe their access to information is being blocked or otherwise infringed? Citizen consultations on such issues as well as the use of user-generated tools would better enable users to voice their opinions and participate in processes shaping the future of the Internet.

Dissemination of Good Practice

The right to freedom of expression is often tempered by the prohibition of certain actions or content, such as hate mail or video, and music mashes. Organizations like the UNESCO should facilitate efforts to develop a set of guidelines or principles, which might support good practice in the regulation of freedom of expression and connection. In other words, if such regulation is to occur, we should identify certain core principles that can minimize harm, such as the transparency of practices, the establishment of an independent regulatory body, or the introduction of rights of appeal for blacklisted sites. This report illustrates that freedom of expression and connection must often be balanced with competing values and interests. In many cases, there are real conflicts of interests that cannot be resolved simply by greater transparency, but only by judicial, legislative or other political processes that arbitrate these differences.

Promoting Balanced versus Absolute Positions in the Global Arena

It is important to explore and promote discussion on a balance between freedom of expression and other core rights in the online world, such as intellectual property, privacy or child protection. There is variation across nations and cultures in the priority placed on different values and interests. An acceptable balance, locally and globally, is not only important in principle, but

is also pragmatically significant to the future vitality of the Internet. On issues where there is most international agreement (e.g. in prevention of child abuse and blocking the dissemination of child abuse images), discussion should be opened up to all stakeholders to explore the best solutions in addressing these issues whilst minimizing restrictions on freedom of expression.

Tracking the Technologies of Filtering and Disconnection

The technologies underpinning content filtering and surveillance of users in support of disconnection are advancing and it may be that better tools could enable freedom of expression by more precisely filtering content judged unacceptable by local or national standards. In the early development of filtering technologies, blunt tools for filtering were likely to block entire sources of information, such as a newspaper or website. More sophisticated tools could block only targeted material. For example, if a symbol like the swastika is illegal to publish in Germany, should filtering technology be able to specifically identify text with this symbol, filter the symbol, and not block all content from the offending source? Historically, filtering mostly meant either over-blocking sites which are not meant to be filtered or under-blocking them, by missing sites that were intended to be blocked (Deibert 2008). More accurate filters could enable better communication to occur and allow nations to be more secure and national values to be respected. Alternatively, more sophisticated filtering technologies could encourage greater use of filtering in a wider array of areas. Regardless of the impact of these technologies, it is important to track their development as a means to inform and stimulate debate about their use.

Driving Corporate Social Responsibility

Related to this is the need to support and promote responsible behaviour amongst non-state actors, in particular in business and industry. Given that many of the biggest technology companies play a significant role in providing Internet services in countries where freedom of expression is limited, UNESCO should consider ways to encourage these corporations to act in a socially responsible manner, without requiring them to act illegally. The Global Network Initiative is one such effort that seeks to provide a set of guiding principles for its members. Many corporations such as Yahoo! and Google have already signed up (http://www.globalnetworkinitiative.org/index.php). Alternatively, a smaller scale option might be to work with industry bodies (such as EuroISPA) to discuss, promote and reward responsible behaviour within Internet related sectors.

Identifying and Stimulating Debate on Key Issues

Given its international status, UNESCO is well placed to host and shape debate around some of the tougher challenges in confronting freedom of speech online. One of the most divisive topics is the proper extent of balancing intellectual property rights of digital material with complementary and competing rights. This is clearly an issue on which UNESCO already has significant expertise, and where it is well-placed to bring together stakeholders

from creative industries, performer or artists' groups, as well as user groups, to consider how measures are currently promoting or limiting freedom of expression online.

Broadening Involvement with Internet Governance and Regulation

Internet governance and regulation is at times dismissed as marginal or irrelevant to maintaining and enhancing the role of the Internet in society, because it is identified with a few Internet policy areas such as the assignment of domain names. However, the potential significance of Internet governance and regulation – if properly conceptualized – is great. It not only concerns these Internet policy issues, but also issues concerning the behaviour of users, such as with respect to fraud, and broad telecoms and regulatory issues that shape Internet use, such as copyright.

All stakeholders in the Internet should encourage the Internet Governance Forum to broadly define Internet governance in order to include the full range of issues shaping the design and use of the Internet and its societal implications. At the same time, stakeholders should increase the priority they place on Internet governance and regulatory processes. Internet governance and regulation will progressively shape information and communication access in all arenas around the world. This is no time for complacency or nation-centric activities, but rather for a greater focus on global governance.

Fostering Further Research

This report was based on a critical review of existing research, with the aim of placing the discussion of freedom of expression into a broader and more realistic framework that can guide further policy-relevant research. The authors hope that this framework, along with the full report, will form a basis for soliciting the views of a wider community of legal scholars, rights advocates, and researchers. Additional investigation, augmented by these discussions, should be fostered in ways that stimulate and inform debate on one of the most critical issues of the digital age.

There is first a need to continue and extend existing efforts to monitor the many and varied trends in law, regulation and opinions highlighted in this report. This synthesis offers a snapshot at a specific point in time, which although it draws on historical trends, illustrates that the evolving nature of these legal and regulatory landscapes is fast paced. It is essential that the legal and regulatory ecology of the Internet be tracked in a more systematically global, rigorous and sustained manner.

More generally, it is important to place Internet freedom of expression and connection in a broader context of allied values and interests, such as privacy and diversity. The framework of this report is offered as a first step for the development of a broader foundation for the study of Internet freedom – one that can stimulate and inform debate over Internet governance and regulation, shaping freedom of expression and connection whilst ensuring the protection of citizens and fundamental rights.

Appendix 1. Glossary

ARPAnet	The first packet switching network, and the preliminary version of the Internet, invented by the Defence Advanced Research Projects Agency (DARPA) of the US Department of Defence.
ASCII	The American Standard Code for Information Interchange (ASCII) is an character-encoding scheme based on the order of the English alphabet. Its numerical codes represent text in computers and communication equipment and have been used by most modern schemes for character encoding.
Blog	A website, usually maintained by a person with regular entries of commentary, descriptions of happenings, graphics or video. The ability of readers to leave comments in an interactive format is an important part of many blogs.
Clean feed	The name given to privately administered content filtering systems on an ISP level in the UK and Canada. It is also the name of a proposed mandatory Australian content filtering system. They are mandated by governments and try to block access to web pages containing (child-) pornography, which are located outside of the country operating the filtering system.
Committee to Protect Journalists	A NGO based in New York, which promotes freedom of the press and defends the rights of journalists. It was founded in 1981 by a group of American foreign correspondents in response to harassment from authoritarian governments.
Computer virus	A code that copies itself in ways that could harm a computer system, such as by slowing its operation
Denial-of-service	A denial-of-service attack aims to make a computer resource unreachable. Usually this is done by saturating the target machine with a huge amount of communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable.
Deep Packet Inspection	The use of computer systems that can inspect packets sent over networks using Internet Protocol in ways that

enable a third party, not the sender or receiver, to identify particular aspects of the communication.

Digital Rights Management
: A generic term for access control technologies that aim to control access and can be used by publishers, copyright holders and companies trying to enforce limited usage of digital content. Sometimes it is also called Digital Restrictions Management.

Domain Name System
: Translates the commonly used alphabetic version of a domain name into its numerical IP address.

Dot-com bubble
: A speculative financial period between 1995–2000 (with a climax on March 10th 2000 when the NASDAQ peaked at 5132.52) during which equity values in stock markets rose rapidly in the Internet sector and related fields.

End-to-end-principle
: The central design principles of the Internet, which is implemented in the design of the underlying methods and protocols. It says that communications protocol operations should be defined to occur at the end-points of a communications system, or as close as possible to the resource being controlled.

File sharing
: The practice of distributing or providing access to digitally stored information (i.e. computer programs, audio, video, documents) to other users.

Freedom House
: An independent NGO that undertakes international monitoring and advocacy of civil liberties. www.freedomhouse.org

Freedom of Expression
: The right to freedom of expression (freedom of speech) is recognized as a human right under Article 19 of the Universal Declaration of Human Rights and recognized: ‘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 Information
: The right to freedom of information refers to the protection of the right to freedom of expression by protecting the right to seek and receive any information. It

	can also refer to the Freedom of Information Act, which is the legal right, subject to certain exclusions, of the public, to access and correct public records in the UK. With regards to the Internet and information technology Freedom of information may also concern censorship, i.e. the ability to access digital content on the Internet.
Global Network of Societies Project	The Global Network of Societies (GNS) Project joins together an international group of researchers to explore the relationships between networks and societies around the world. It takes as its initial position the hypothesis that the Internet is indeed being used in ways that are transforming societies, but in ways that are shaped by the diversity of world cultures - the sets of beliefs and values that underpin the strategic and non-strategic use of ICTs by individuals, organizations and networks. (http://www.oii.ox.ac.uk/research/?id=46)
Global Voices	A citizen media network http://globalvoicesonline.org/
Green dam	A content-control software developed under a directive from the Chinese Ministry of Industry and Information Technology. It is mandatory to have either the software, or its setup files accompanied on a compact disc or pre-installed on all new computers sold in China. http://en.wikipedia.org/wiki/Green_Dam - cite_note-2
IANA	An organization that oversees IP address, Top-level domain and Internet protocol code-point allocations.
ICANN	A California-based non-profit corporation charged with the responsibility to assign names and numbers to keep the Internet secure, stable and interoperable.
ICT	A generic name for the technologies involved in communicating with computers and digital media.
IGF	The Internet Governance Forum supports the UN Secretary-General in carrying out the mandate from the WSIS to convene a forum for multi-stakeholder policy dialogue.
Information age	The period from the last quarter of the 20th century when information became more easily accessible through computers and computer networks.
Information society	A society connected by complex communication networks that quickly develops and exchanges information.

Internet backbone	Refers to the principle data routes in the Internet between large, strategically interconnected networks and core routers, which are hosted by commercial, government, academic and other high-capacity network centres.
Internet filtering	A government, an Internet Service Provider, a company or a parent can install software, either on a personal computer at home or on a server in an organization that restricts content to users. A filter can screen particular words, email addresses, Web sites or other addresses and be used, for example, if a country wishes to prevent users within its borders from seeing a particular news site online.
Internet Governance	The development and application by Governments, the private sector and civil society of shared principles and rules that shape the evolution and use of the Internet.
Internet Protocol	Standards used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as TCP/IP.
Internet Watch Foundation	A NGO based in the United Kingdom, which offers an online service for the public to report content on the Internet that is considered to be "potentially illegal".
Internet server	A computer configured to be left on and constantly connected to the Internet. Any Internet user in the world can access Web sites accessible on, or linked to, the server.
IPv4	The fourth revision in the development of IP, and the first protocol to be widely deployed. See IPv6.
IPv6	IP version 6, the next generation version of IP. It increases the address space from 32 to 128 bits, providing for a vast number of networks and systems.
ISP	Internet Service Provider. Companies that offer customers access to the Internet.
ITU	International Telecommunication Union. UN body coordinating international telecommunications standards and policy.

Libel Tourism	People who feel defamed by a (digitally available) publication can, in the right circumstances, bring a lawsuit against a publisher or author to the country in which the complainant it is likely to obtain a more favourable ruling. (see Box 8.1)
MacBride Commission	A commission, which was established in 1977 by UNESCO, and reported in 1980 with the publication of *Many Voices One World* (ICCP 1980), which came to be known as the MacBride Report. This became a major reference for advocacy of a 'New World Information and Communication Order' (NWICO). (see Box 1.1)
Malware	Software designed to damage computers or computer systems, such as by installing a computer virus.
Media literacy	The ability to access, analyze, evaluate, and produce communication and information in a variety of forms and means (http://www.unesco.org/education/educprog/lwf/doc/portfolio/definitions.htm).
P2P	A peer-to-peer distributed network architecture built up by participants by providing resources (such as processing power or network bandwidth) to other network participants, without the need for central nodes such as servers or stable hosts.
RSS	A variety of web feed formats used to publish frequently updated works (e.g. news headlines). An RSS feed includes text and metadata such as publishing dates and authorship.
Skype	A software application that allows users to make voice calls, instant messaging, file transfer and video conferencing over the Internet.
Social network service	A web-based service that provides tools to build social networks or social relations among people. A social network service basically contains a profile or representation of each user, his/her social links, and a variety of additional services (e.g. facebook.com).

Spam	Bulk unwanted email that may contain malware.
Top Level Domain	The highest level of domain names in the DNS.
Twitter	A free social networking and micro blogging service that enables users to send and read messages known as tweets.
User-generated content	Any kind of media content that is publicly available and produced by end-users.
Voice over IP	A variety of transmission technologies for delivery of voice communications over the Internet or other packet-switched networks.
Web 1.0	Communication enabled by the web focusing on sharing Information (hypertextual links on the Web, enabling the global sharing of documents, text, video, etc.) (see table 1)
Web 2.0	Communication enabled by the web focusing on user-generated content (Blogging, micro-blogging (e.g., Twitter), user comments, ratings, polling, etc.) (see table 1)
Web 3.0	Communication enabled by the web focusing on co-creation or co-production of information (see table 1)
WGIG	Working Group on Internet Governance. It was a UN multi-stakeholder working group set up after the 2003 WSIS to agree on the future of Internet governance.
WIPO	World Intellectual Property Organization
WSIS	World Summit on the Information Society. It was a pair of UN-sponsored conferences about information, communication and the information society. Held in 2003 in Geneva and in 2005 in Tunis.

Appendix 2. Abbreviations and Acronyms

ARPAnet	Advanced Research Projects Agency Network
AT&T	American Telephone & Telegraph Corporation
ccTLD	Country Code Top-Level Domain
CEJA-JSAC	Justice Studies Centre of the Americas
CIPA	Children Internet Protection Act
CPJ	Committee to Protect Journalists
CSTD	Commission on Science and Technology for Development
DMCA	Digital Millennium Copyright Act
DNS	Domain Name System
DPI	Deep Packet Inspection
DRM	Digital Rights Management
ECHR	The European Convention on Human Rights (formally the Convention for the Protection of Human Rights and Fundamental Freedoms)
EoG	Ecology of Games
EuroISPA	European Association of European Internet Services Providers
FCC	Federal Communications Commission
FH	Freedom House
FoE	Freedom of Expression
FoI	Freedom of Information
FOSS	Free and Open Source Software Policy
GAID	Global Alliance for ICT for Development
IANA	The Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICCPR	International Covenant on Civil and Political Rights

ICESCR	International Covenant on Economic, Social and Cultural Rights
ICT	Information and Communication Technologies
ICTD	ICT for Development, also ICT4D
IDN	Internationalized Domain Names
IGF	Internet Governance Forum
IGIF	Index of Global Internet Freedom
IP	Internet Protocol
IPR	Intellectual Property Rights
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISP	Internet Service Provider
ITU	International Telecommunication Union
IWF	Internet Watch Foundation
MIC	Vietnam Ministry of Information and Communications
NGO	Non-Governmental Organization
NWICO	New World Information and Communication Order
P2P	Peer-to-Peer
R & D	Research and Development
RIM	Research in Motion
RSS	Really Simple Syndication
SNS	Social Network Service
SPAM	Unwanted and unsolicited electronic communication
TLD	Top Level Domains
TRIPS	Trade Related Aspects of Intellectual Property Rights
UDHR	Universal Declaration of Human Rights

UGC	User-Generated Content
UNESCO	United Nations Educational, Scientific and Cultural Organization
URI	Universal Resource Identifier
URL	Uniform Resource Locator
VoA	Voice of America
VoIP	Voice over Internet Protocol
W3C	World Wide Web Consortium
WCT	WIPO Copyright Treaty
Web	World Wide Web
WGIG	Working Group on Internet Governance
WIP	World Internet Project
WIP2	World Internet Policy Project
WIPO	World Intellectual Property Organization
WPFC	World Press Freedom Committee (merged with FH in 2009)
WPPT	WIPO Performances and Phonograms Treaty
WSIS	World Summit on the Information Society

Appendix 3 List of Tables and Figures

Tables

Figures

References

Abida, M. (2009). 'Case study: The World Summit on the Information Society - A reflection', in *ICT4D: Information and Communication Technology for Development*, Tim Unwin (ed.), Cambridge: Cambridge University Press, 142-143.

Abril, A. (2006). 'Mitos y realidad del gobierno de Internet', IDP Revista de los Estudios de Derecho y CienciaPolítica de la UOC, 3 (2006). Available at www.uoc.edu/idp

Access to Knowledge - Copyright as a Barrier to Accessing Books, Journals, and Teaching Material. (2004). Retrieved from http://www.idrc.ca/en/ev-67263-201-1-DO_TOPIC.html

ACHPR (1981). African Charter on Human and Peoples' Rights, adopted at Nairobi, Kenya (1981). Retrieved from http://www.achpr.org/english/_info/charter_en.html

ACHPR (2002). African Commission on Human and Peoples' Rights, *Declaration of Principles on Freedom of Expression in Africa*, adopted 2002: http://www.achpr.org/english/declarations/declaration_freedom_exp_en.html

ACHR (1969). American Convention on Human Rights, adopted at San José, Costa Rica, 22 November (1969). Available at http://www.oas.org/juridico/English/treaties/b-32.html

Aguerre, C. and Guillermo Mastrini (2009). "Regional Report: Latin America". Global Information Society Watch 2009. Ed. Alan Finlay. Uruguay: APC and HIVOS.

Amnesty International. "Shi Tao, 10 Years in Prison for Sending an Defence." Retrieved on January 15, 2010 from http://www.amnestyusa.org/individuals-at-risk/priority-cases/china-shi-tao/page.do?id=1101243

Anderson, Kevin. "Google and China: superpower standoff", *Guardian.co.uk*, January 13th, 2010. Retrieved on January 15, 2010 from http://www.guardian.co.uk/technology/blog/2010/jan/13/google-china-hacking-twitter-bloggers

Anestopoulou, M. and McKenna, A. (2001). 'Country Report-Greece'. The APC European Internet Rights Project. Retrieved on October 10, 2010 from http://europe.rights.apc.org/c_rpt/greece.html

Argüero, M.R. (September 7, 2010). 'Acceso a Internet es un derecho fundamental'. La Nación/El país. Retrieved on October 12, 2010 from http://www.nacion.com/2010-09-08/ElPais/NotasSecundarias/ElPais2514038.aspx

Atkinson, R. D., & Weiser, P. (2006). A 'Third Way' on Network Neutrality. *SSRN eLibrary*.

Avgerou, C., Smith, M. L., & Besselaar, P. V. D. (Eds.). (2008). *Social Dimensions of Information And Communication Technology Policy, Proceedings of the Eighth International Conference on Human Choice and Computers (HCC8), IFIP TC 9, Pretoria, South Africa, September 25-26, 2008*. IFIP (Vol. 282). Springer.

Baer, W. S. (1996). 'Telecommunication Infrastructure Competition: The Costs of Delay' in Dutton (1996): 353-70.

Baer, W. S., Borisov, N., Danezis, G., Dutton, W. H., Guerses, S. F., Klonowski, M., Kutylowski, M., Maier-Rabler, U., Moran, T., Pfitzmann, A., Preneel, B., Sadeghi, A-R.,Vedel, T., Westen, T., and Zagorski, F., (2009),'Machiavelli Confronts 21st Century Digital Technology: Democracy in a Network Society', OII Working Paper (Oxford: Oxford Internet Institute: University of Oxford): December. Available at SSRN: http://ssrn.com/abstract=1521222

Bailey, C. (2006), "Strong copyright + DRM + weak net neutrality=digital dystopia?", Information Technology and Libraries, Vol. 34 No.3, pp.116-127, 139. Available at http://www.ftrf.org/ala/mgrps/divs/lita/ital/252006/number3september/bailey.pdf

Balkin, J. M. (2004). Digital Speech and Democratic Culture: a Theory of Freedom of Expression for the Information Society. *New York University Law Review, Vol. 79, No. 1, 2004*. Available at doi: 10.2139/ssrn.470842

Balkin, J. M. (2009). The Future of Free Expression in a Digital Age.*Pepperdine Law Review, Vol. 36, 2008*.

Bambauer, D. E. (2008a). Cybersieves. *Duke Law Journal, Vol. 59, 2009*.

Bambauer, D. E. (2008b). Filtering in Oz: Australia's Foray into Internet Censorship. *SSRN eLibrary*. Retrieved December 31, 2009, from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1319466

BBC (2010). British Broadcasting Corporation, 'Four in Five Regard Internet Access as a Fundamental Right: Global Poll'. Available at http://news.bbc.co.uk/1/hi/technology/8548190.stm

BBC. (2010). 'Finland makes Broadband a 'Legal Right', BBC News Technology, 1 July. Retrieved on October 10, 2010 from http://www.bbc.co.uk/news/10461048

Bell, D. (1974), *The Coming of Post-Industrial Society* (London: Heinemann; originally published, New York: Basic Books, 1973).

Benkler, Y. (2006). *The wealth of networks : how social production transforms markets and freedom*. New Haven [Conn.]: Yale University Press.

Berleur, J. (2008). 15 years of ways of Internet governance: Towards a new agenda for action. In *Social Dimensions Of Information And Communication Technology Policy* (pp. 255-274). Retrieved from http://dx.doi.org/10.1007/978-0-387-84822-8_17

Berleur, J., &Poullet, Y. (2006). What Governance and Regulations for the Internet? Ethical Issues. In *The Information Society: Emerging Landscapes* (pp. 169-191). Retrieved on December 30, 2009, from http://dx.doi.org/10.1007/0-387-31168-8_11

Berlingieri, E (2010). "The Google Trial in Italy: the motivation behind the conviction", posted on Elvlog, April 18th, 2010. Retrieved on May 21, 2010 from http://elvlog.wordpress.com/2010/04/18/the-google-trial-in-italy-the-motivation-behind-the-conviction/

Bernstorff, J. V. (2003). Democratic Global Internet Regulation? Governance Networks, International Law and the Shadow of Hegemony. *European Law Journal*, *9*(4), 511-526. Available at doi: 10.1111/1468-0386.00189

Best, B. (2010). *Understanding our Knowledge Gaps: Or, Do we have an ICT4D field? And do we want one?,* Publius Project, February 5th, 2010. Retrieved on March 2, 2010 from http://publius.cc/understanding_our_knowledge_gaps_or_do_we_have_ict4d_field_and_do_we_want_o

Bhasin, M. L. (2006). Guarding Privacy on the Internet. *Global Business Review*, *7*(1), 137-156. Available at doi: 10.1177/097215090500700109

Brazilian Court Bans P2P Software | TorrentFreak. (n.d.). Retrieved from http://torrentfreak.com/brazilian-court-bans-p2p-software-090918/

Bremner, C. (July 11, 2009). 'Top French court rips heart out of Sarkozy internet law'. *Times Online*. Retrieved on October 10, 2010 from http://technology.timesonline.co.uk/tol/news/tech_and_web/article6478542.ece

Brenner, S. W., (2007). 'Should Online Defamation Be Criminalized?', *Mississippi Law Journal*, Vol. 76, 2007. Retrieved on February 8, 2010 from http://ssrn.com/abstract=982418

Bright, A. (2010). "Will Italy's Conviction of Google Execs Stick?", Citizen Media Law Project Blog, March 2nd, 2010. Retrieved on March 3, 2010 from http://www.citmedialaw.org/blog/2010/will-italys-conviction-google-execs-stick?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+CitizenMediaLawProject+%28Citizen+Media+Law+Project%29

Brown, I. (2007). Internet Filtering - Be Careful What You Ask for. *SSRN eLibrary*.

Brown, I. (2008). Regulation of Converged Communications Surveillance. *New Directions in Surveillance and Privacy, D. Neyland and B. Goold, eds., pp. 39-73, Exeter: Willan, 2009*.

Brown, I. (2010). 'Beware Self-Regulation', *Index on Censorship*, Vol. 39, No 1: 98-106.

Brown, I., & Korff, D. (2008). Terrorism and the Proportionality of Internet Surveillance.*European Journal of Criminology, Vol. 6, No. 2, pp. 119-134, 2009*.

Burgman, C. et al. (2008). *Our Rights, Our Information: Empowering People to Demand Rights through Knowledge, in* MajaDaruwala and VenkateshNayak (eds). Commonwealth Human Rights Initiative. Retrieved on January 31, 2010 from http://www.accessinitiative.org/resource/our-rights-our-information

Callanan, C. et al. (2009). Internet blocking balancing cybercrime responses in democratic societies. Prepared within the framework of Open Society Institute funding. Available at http://www.aconite.com/sites/default/files/Internet_blocking_and_Democracy.pdf

Calo, R (2010). "Google & Privacy: Not what you might think", posted on The Center for Internet and Society, Standford Law School, March 17, 2010. Retrieved on May 21, 2010 from http://cyberlaw.stanford.edu/node/6443

Cammarano, P. (2002). Internet and the Censorship: Is it Legal (And Necessary) to Censor the Web? *SSRN eLibrary*. Available at doi: 10.2139/ssrn.346861

Canaves, Sky. “China Real Time Report: Clearing Up Confusion on Google and China”, The Wall Street Journal. January 15, 2009. Retrieved on January 15, 2010 from http://blogs.wsj.com/chinarealtime/2010/01/15/clearing-up-confusion-on-google-and-china/

Castells, M. (2000, 1996). The Rise of the Network Society, 2nd Edition (Blackwell Publishers: Oxford).

Castells, M. (2001). The Internet Galaxy (Oxford University Press: Oxford).

Castells, M. (ed.) (2005). The Network Society: A Cross-Cultural Perspective (Edward Elgar Publications: Northampton, MA).

Castells, M. (2009), *Communication Power*. Oxford: Oxford University Press.

Castells, M. and Himanen, P. (2004). The Information Society and the Welfare State: The Finnish Model (Oxford University Press: Oxford).

CEJA-JSCA (2009). Centro de EstudiosJusticia de lasAméricas, *Índices de accessibilidad a la información judicial en Internet*. 5th edition. Retrieved on January 31, 2010 from http://www.cejamericas.org/cejacommunity/apl/prodespeciales/menuprodespecial.php?evento=97

Cheng, H. K., Bandyopadhyay, S., &Guo, H. (2008). The Debate on Net Neutrality: A Policy Perspective. *Information Systems Research* - Forthcoming.
Children's welfare groups slam net filters - Technology - theage.com.au (n.d.). Retrieved from http://www.theage.com.au/articles/2008/11/28/1227491813497.html?page=fullpage

Chima, R. J. (2008). The Regulation of the Internet With Relation to Speech and Expression by the Indian State.*SSRN eLibrary*.

China's Green Dam: The Implications of Government Control Encroaching on the Home PC | OpenNet Initiative. (n.d.). Retrieved from http://opennet.net/chinas-green-dam-the-implications-government-control-encroaching-home-pc

Clayton, R., Murdoch, S., & Watson, R. (2006). Ignoring the Great Firewall of China. In *Privacy Enhancing Technologies* (pp. 20-35). Retrieved on December 31, 2009 from http://dx.doi.org/10.1007/11957454_2

Clinton, H. R. (2010). ‘Internet Freedom: The prepared text of U.S. of Secretary of State Hillary Rodham Clinton's speech, delivered at the Newseum in Washington, D.C., 21 January. Available at http://www.foreignpolicy.com/articles/2010/01/21/internet_freedom?page=full

Copyright policy alternatives for preserving end-user freedom of expression and information. (2008). In *EU Digital Copyright Law and the End-User* (pp. 233-283). Retrieved on December 31, 2009 from http://dx.doi.org/10.1007/978-3-540-75985-0_8

de Sola Pool, I. (1983). *Technologies of Freedom*. (Cambridge, Mass.: Harvard University Press, Belknap Press).

deVries, S. (2005). Public service, diversity and freedom of expression and competition law.*ERA-Forum*, *6*(1), 46-57. Available at doi: 10.1007/s12027-005-0043-z

Deibert, R. J. (2002). Dark Guests and Great Firewalls: The Internet and Chinese Security Policy. *Journal of Social Issues*, *58*(1), 143-159. Available at doi: 10.1111/1540-4560.00253

Deibert, R. J., Palfrey, J. G., Rohozinski, R., and Zittrain, J. (2008) (Eds), *Access Denied: The Practice and Policy of Global Internet Filtering*. (Cambridge, Mass.: MIT Press).

Deibert, R. J, Palfrey, J. G., Rohozinski, R., and Zittrain, J. (2010) (eds), *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*. (Cambridge, Massachusetts: MIT Press).

Deutsch-Karlekar, Karin and Sarah G. Cook (2009). Access and control: A growing diversity of threats to Internet freedom. Available at http://www.freedomhouse.org/uploads/specialreports/NetFreedom2009/FOTN%20Overview%20Essay.pdf

Deva, S. (2007). Corporate Complicity in Internet Censorship in China: Who Cares for the Global Compact or the Global Online Freedom Act? *George Washington International Law Review, Vol. 39, pp. 255-319, 2007*.

Dreyfuss, R. C., Zimmerman, D. L., & First, H. (2001). *Expanding the boundaries of intellectual property*. Oxford University Press.

Drummond, D. “A New Approach to China”, posted on the Official Google Blog on January 12, 2010. Retrieved on January 15, 2010 from http://googleblog.blogspot.com/

Duffy, M. E. (2003). Web of Hate: a Fantasy Theme Analysis of the Rhetorical Vision of Hate Groups Online. *Journal of Communication Inquiry*, *27*(3), 291-312. Available at doi: 10.1177/0196859903252850

Dutton, W. H. (1992). The Ecology of Games Shaping Telecommunications Policy. *Communication Theory*, *2*(4), 303-328.

Dutton, W. H. (1996) (ed.), with the assistance of Malcolm Peltu, *Information and Communication Technologies – Visions and Realities*, Oxford and New York: Oxford University Press.

Dutton, W.H. (1999). Society on the Line (Oxford University Press: Oxford).

Dutton, W.H. (2004). *Social Transformation in the Information Society*(UNESCO Series for the WSIS: Paris). Available at http://portal.unesco.org/ci/en/ev.php-URL_ID=12848&URL_DO=DO_TOPIC&URL_SECTION=201.html

Dutton, W. H. (2005). ‘The Internet and Social Transformation: Reconfiguring Access,’ pp. 375-97 in Dutton, W. H., Kahin, B., O’Callaghan R., and Wyckoff, A. W. (eds.), *Transforming Enterprise,* Cambridge, MA: MIT Press.

Dutton, W. H. (2008). 'Social Movements Shaping the Internet: The Outcome of an Ecology of Games', Chapter 19, pp. 499-517 in Elliott, M. and Kraemer, K. L. (eds), *Computerization Movements and Technology Diffusion: From Mainframes to Ubiquitous Computing*. Medford, NJ: Information Today, Inc.

Dutton, W. H. (2009). 'The Fifth Estate Emerging through the Network of Networks', *Prometheus*, Vol. 27, No. 1, March: pp. 1-15.

Dutton, W. H., and Peltu, M. (2007). 'The Emerging Internet Governance Mosaic: Connecting the Pieces', *Information Polity*, 12: 63-81. An earlier working paper is available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1295330

Dutton, W. H. and Jeffreys, P. W. (2010). *World Wide Research: Reshaping the Sciences and Humanities*. (Cambridge, MA: MIT Press).

Dutton, W. H., Schneider, V., &Vedel, T. (2008). Large Technical Systems as Ecologies of Games: Cases from Telecommunications to the Internet. *SSRN eLibrary*.

Dutton, W.H., Kahin, B., O'Callaghan, R. and Wyckoff, A.W. (eds) (2005). Transforming Enterprise (MIT Press: Cambridge, MA).

ECHR (1950), *European Convention on Human Rights.* Available at http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm

Edwards, L. (2009). Pornography, Censorship and the Internet. *SSRN eLibrary*.

Erdos, D. (November 12, 2009). Research Fellow at the Centre for Socio-Legal Studies. Oxford University. Interview.

Espinosa, C. A. (2009).'Network Information and the Principle of Technological Neutrality: The Freedom of Expression and Dissemination of Administrative Information' (La Información En La Red Y El Principio De NeutralidadTecnológica: La Libertad De Expresión Y La Difusión De InformaciónAdministrativa),*RevistaDerecho del Estado No. 22*. Available at SSRN: http://ssrn.com/abstract=1476887

Faris, R., and Villeneuve, N. (2008), 'Measuring Global Internet Filtering', pp. 5-27 in Deibert, R., Palfrey, J., Rohozinski, R., and Zittrain, J. (eds), *Access Denied: The Practice and Policy of Global Internet Filtering*. (Cambridge, Mass: MIT Press).

Faris, R., Wang, S., & Palfrey, J. (2008). Censorship 2.0. *Innovations: Technology, Governance, Globalization*, *3*(2), 165-187.

Finnish Ministry of Transport and Communications. (June 29, 2010). '1 Mbit Internet access a university service in Finland from the beginning of July'. Press Release. Finnish Government. Retrieved on October 10, 2010 from http://www.valtioneuvosto.fi/ajankohtaista/tiedotteet/tiedote/en.jsp?oid=301979

Fisher, W. (2001*a*). 'Theories of Intellectual Property', pp. 168-200, in S. R. Munzer (ed.), *New Essays in the Legal and Political Theory of Property* (Cambridge: Cambridge University Press).

Fisher, W. (2001*b*). Freedom of Expression on the Internet. Available at http://cyber.law.harvard.edu/ilaw/Speech/

Freedom of Use vs DRM Technology. (2008). In *EU Digital Copyright Law and the End-User* (pp. 179-229). Retrieved on December 31, 2009 from http://dx.doi.org/10.1007/978-3-540-75985-0_7

Freedom House (2008), 'Index of Global Internet Freedom (IGIF) – Pilot Study', presentation at Internet Governance Forum, Hyderabad, India, December. Available at http://www.slideshare.net/netfreedom/igf-hyderabad-index-of-global-Internet-freedom-presentation

Freedom House (2009). Freedom on the Net: A Global Assessment of Internet and Digital Media. (Freedom House).

Gasser, U. (n.d.). Copyright and Digital Media in a Post-Napster World: International Supplement. *SSRN eLibrary*. Available at doi: 10.2139/ssrn.655391.

Geist, M. (2009). Michael Geist - B.C. Court of Appeal Rules No Liability For Linking. Retrieved December 31, 2009, from http://www.michaelgeist.ca/content/view/4393/125/.

Gey, S. G. (2000). Fear of Freedom: The New Speech Regulation in Cyberspace. *SSRN eLibrary*. Available at doi: 10.2139/ssrn.220410.

Global Network Initiative - Principles. (n.d.). Available at http://www.globalnetworkinitiative.org/principles/index.php

Graux, H. (2009). Darknets and the Future of Freedom of Expression in the Information Society. In *Facing the Limits of the Law* (pp. 1-22). Retrieved on December 30, 2009 from http://dx.doi.org/10.1007/978-3-540-79856-9_24

Gurumurthy, A. (2009). *Social Entreprise to Mobiles- The Curious Case of a Propped up ICTD Theory*, Publius Project: Berkman Centre for Internet & Society, September 17th, 2009. Retrieved on March 2, 2010 from http://publius.cc/social_enterprise_mobiles_%E2%80%93_curious_case_propped_ictd_theory/091709

Hamilton, S. (2004). *To what extent can librairies ensure free, equal and unhampered access to Internet-accessible information resources from a global perspective?* Copenhagen: Department of Library and Information and Management, Royal School of Library and Information Science/FAIFE. Retrieved on January 31, 2010 from http://ifla.queenslibrary.org/faife/news/2005/Free-equal-accessInternet05.htm

Herman, E. S., McChesney, R. (2001). *The Global Media: The New Missionaries of Corporate Capitalism*. (New York: Continuum).

Hogendorn, C. (2007). Broadband Internet: net neutrality versus open access. *International Economics and Economic Policy*, *4*(2), 185-208. Available at doi: 10.1007/s10368-007-0084-6

Hugenholtz, Bernt (2001). Copyright and Freedom of Expression in Europe. Rochelle Cooper Dreyfuss, Diane Leenheer Zimmerman & Harry First (eds.), Expanding the Boundaries of Intellectual Property. Innovation Policy for the Knowledge Society, Oxford: Oxford University Press. Available at http://www.ivir.nl/publications/hugenholtz/PBH-Engelberg.doc

Hull, G. (2008). Overblocking Autonomy: The Case of Mandatory Library Filtering Software. *Continental Philosophy Review, Vol. 42, pp. 81-100, 2009*.

IACHR (2000), Inter-American Commission on Human Rights, *Inter-American Declaration of Principles on Freedom of Expression.* Available at http://www.iachr.org/declaration.htm

IACHR (2009), The right of access to information Special Rapporteurship for freedom of expression. Available at http://www.oas.org/DIL/access_to_information_IACHR_guidelines.pdf

ICCP *(1980),*International Commission for the Study of Communication Problems, chaired by Sean MacBride,*Communication and Society Today and Tomorrow: Many Voices One World: Towards a new more just and more efficient world information and communication order* (Paris: UNESCO).

Intellectual Property Watch » Blog Archive » Germany Builds Infrastructure To Block The Internet. (2009, June 19). Retrieved on December 31, 2009 from http://www.ip-watch.org/weblog/2009/06/19/germany-builds-infrastructure-to-block-the-Internet/.

ITU (2010). *Measuring Information Society 2010: ITU-D*, Geneva: 2010.

Kakungulu-Mayambala, Ronald (2008): Internet censorship and Freedom of Expression: A critical appraisal of the regulation of hate speech on the Internet. Available at http://www.bileta.ac.uk/Document%20Library/1/Internet%20Censorship%20and%20Freedom%20of%20Expression%20%5BRonald%20Kakungulu%5D.pdf

Karlekar, K. D., and Cook, S. G. (2009). 'Access and Control: A Growing Diversity of Threat to Internet Freedom', an overview essay in Freedom House (ed), *Freedom on the Net* (Freedom House): 1-12. Available at http://www.freedomhouse.org/template.cfm?page=384&key=194&parent=19&report=79

Kesan, J., and Gallo, A. (2006). Why are the United States and the European Union failing to regulate the Internet efficiently? Going beyond the bottom-up and top-down alternatives. *European Journal of Law and Economics*, *21*(3), 237-266. Available at doi: 10.1007/s10657-006-7422-y.

Khatchadourian, R. (2010). 'No Secrets: Julian Assange's Mission for Total Transparency', *The New Yorker*, 7 June. Available at http://www.newyorker.com/reporting/2010/06/07/100607fa_fact_khatchadourian

Klang, M., and Murray, A. (2005).*Human rights in the digital age*. Routledge Cavendish.

Lessig, L. (1999). *Code and other laws of cyberspace*. New York: Basic Books.

Lessig, L. (2004). *Free culture: how big media uses technology and the law to lock down culture and control creativity*. New York: Penguin Press.

Lessig, L. (2008). *Remix : making art and commerce thrive in the hybrid economy*. New York: Penguin Press.

Livingstone, S. and Haddon, L. (2009). *EU Kids Online: final report*. EU Kids Online, London, UK. Available at http://eprints.lse.ac.uk/24372/

Long N. E. (1958). 'The Local-Community as an Ecology of Games', *American Journal of Sociology*, 64:251-61.

Lungescu, O. (April 7, 2010). 'Tiny Estonia leads internet revolution'. BBC News Channel. Retrieved on October 10, 2010 from http://news.bbc.co.uk/1/hi/world/europe/3603943.stm

Marsden, C. (n.d.). Net Neutrality and Consumer Access to Content. *SSRN eLibrary*. Retrieved on December 31, 2009 from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1089063

Maurushat, A., & Watt, R. (2009). Clean Feed: Australia's Internet Filtering Proposal. *Internet Law Bulletin, 2009*.

Mazziotti, G. (2008). *EU Digital Copyright Law and the End-User*. Retrieved on December 30, 2009 from http://dx.doi.org/10.1007/978-3-540-76985-0

MacKinnon, R. "Google Gets on the Right Side of History: No more censored searches to please the Chinese government." The Wall Street Journal, January 13, 2010. Retrieved on January 16, 2010 from http://online.wsj.com/article/SB10001424052748704362004575000442815795122.html

McIntyre, T. J., & Scott, C. D. (2008). Internet Filtering: Rhetoric, Legitimacy, Accountability and Responsibility. *REGULATING TECHNOLOGIES, Brownsword, R., Yeung, K, eds., Oxford, Hart Publishing*.

McLaughlin, Andre "Google in China", posted on The Official Google Blog, January 27, 2006. Retrieved on January 15, 2010 from http://googleblog.blogspot.com/2006/01/google-in-china.html

Mendel, Toby (2003). Freedom of Information: A Comparative Legal Survey, Nueva Delhi: UNESCO, 2003. Available at http://portal.unesco.org/ci/en/files/26159/12054862803freedom_information_en.pdf/freedom_information_en.pdf

Mendal, Tony. (2008, 2003). *Freedom of Information: A Comparative Legal Survey*. 2nd edition. Paris: UNESCO. Available at http://portal.unesco.org/ci/en/files/26159/12054862803freedom_information_en.pdf/freedom_information_en.pdf

MinistériodaCultura - MinC » Reformada lei do direitoautoralprevêcópiaprivada e oficializamashup. (2009, November 10). Available at http://www.cultura.gov.br/site/2009/11/10/reforma-da-lei-do-direito-autoral-preve-copia-privada-e-oficializa-mashup/

Morozov, E. "Doubting the Sincerity of Google's Threat", Foreign Policy, January 13, 2010. Retrieved on January 15, 2010 from http://neteffect.foreignpolicy.com/posts/2010/01/13/doubting_the_sincerity_of_googles_threat

Morris, S. (November 17, 2009). 'Spain govt to guarantee legal right to broadband'. Reuters. Retrieved on October 12, 2010 from http://www.reuters.com/article/idUSLH61554320091117

Moynihan, C. (2009). *'Arrest Puts Focus on Protesters' Testing', The New York Times, 5 October 2009.* Available at *http://www.nytimes.com/2009/10/05/nyregion/05txt.html*

Mulholland, H. (2009). 'Jack Straw Reveals Plan to Reform UK's 'Chilling' Liber Laws', *Guardian*, 2 December. Available at http://www.guardian.co.uk/politics/2009/dec/02/jack-straw-reform-libel-law

Murdock, S. J., and Anderson, R. (2008). *'Tools and Technology of Internet Filtering', pp. 57-72 in* Deibert, R., Palfrey, J., Rohozinski, R., and Zittrain, J. (eds), *Access Denied: The Practice and Policy of Global Internet Filtering*. (Cambridge, Mass: MIT Press).

Nelson, J. I. (2006-09-26). 'How the NSA Warrantless Wiretap System Works', 26 September. Available at http://www.nerdylorrin.net/jerry/politics/Warrantless/WarrantlessFACTS.html

New Essays in the Legal and Political Theory of Property. (2001). Cambridge studies in philosophy and law. Cambridge, UK: Cambridge University Press.

New Zealand to get countrywide filtered Internet. (2009, September 14). Retrieved from http://www.neowin.net/news/main/09/09/14/new-zealand-to-get-country-wide-filtered-Internet

Ng, K. (2005). Spam Legislation in Canada: Federalism, Freedom of Expression and the Regulation of the Internet. *University of Ottawa Law & Technology Journal*, *2*(2), 447-491.

NSA's Warrantless Wiretaps - just the facts. (2006, September 26). Retrieved from http://www.nerdylorrin.net/jerry/politics/Warrantless/WarrantlessFACTS.html

Nunziato, D. C. (2003). Freedom of Expression, Democratic Norms, and Internet Governance. *Emory Law Journal*, *52*, 187.

Nunziato, D. C. (2008). Net Neutrality, Free Speech, and Democracy in the Internet Age. *GWU Law School Public Law Research Paper No. 440*.

O'Neill, S. (2010). 'Government Ban on Internet Firms that do not Block Child Sex Sites', Timesonline, 10 March 2010. Available at http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article7055882.ece

OSCE (2008). Ten Years for Media Freedom - An OSCE Anniversary. Current and Forthcoming Challenges. Available at http://www.osce.org/publications/rfm/2008/09/32993_1179_en.pdf

Palfrey Jr., J. G. (2007). Reluctant Gatekeepers: Corporate Ethics on a Filtered Internet. *GLOBAL INFORMATION TECHNOLOGY REPORT, World Economic Forum, 2006-2007*, 69.

Parmar, V. (2009). *Forum: A Multidisciplinary Approach to ICT Development*, USC

Annenberg School for Communication & Journalism, Volume 5: Number 4, Winter 2009, 89-96.

Preston, C. B. (2007). Zoning the Internet: A New Approach to Protecting Children Online. *Brigham Young University Law Review*, 1417-1467.

Qui, J. L. (2009). *Working-Class Network Society*. Cambridge: MIT Press.

R. L. (2000). Censor dot gov: the Internet and press freedom 2000. *Journal of Government Information*, *27*(5), 537-545. Available at doi: 10.1016/S1352-0237(00)00203-3

RAE (2007), *Royal Academy of Engineering, Dilemmas of Privacy and Surveillance*. London: Royal Academy of Engineering.

Reding, V. (2007). 'The Importance of Freedom of Expression for Democratic Societies in the Enlarged European Union'. Speech given at a press conference on the conclusion of a Framework Agreement between the International Federation of Journalists and WAZ Mediengruppe, 9 July.

Reding, V. (2009). Freedom of speech: ICT must help, not hinder. Speech. EP Plenary Session, Strasbourg, 3 February 2009. Available at http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=4705

Rens, A. J., & Kahn, R. (2009). Access to Knowledge in South Africa: Country Study Version 2.0. *SSRN eLibrary*.

Reporters without Borders (2006). Available at http://www.rsf.org/IMG/pdf/rapport_gb_md_1.pdf

Reporters without Borders (2010). *Enemies of the Internet: Countries Under Surveillance*. Paris: Reporters without Borders. Available at http://www.readwriteweb.com/archives/enemies_of_the_internet_not_just_for_dictators_anymore.php

RISEPTIS (2009). Research and Innovation on Security, Privacy and Trustworthiness in the Information Society, Trust in the Information Society. Available at http://www.think-trust.eu/general/news-events/riseptis-report-published.html

Robertson, S. (2008). 'Was it right to censor a Wikipedia page?' Financial Times, 11 December.

Robertson, S. (2010). 'Google convictions reveal two flaws in EU law, not just Italian law', Op-ed posted on Out-Law.com, March 3, 2010. Retrieved on May 21, 2010 from http://www.out-law.com/page-10805

Rosenberg, R. (2001). Controlling access to the Internet: The role of filtering. *Ethics and Information Technology*, *3*(1), 35-54. Available at doi: 10.1023/A:1011431908368

Rotenberg, M. (2010). "Brandeis in Italy: the Privacy Issue in the Google Video Case", *The Huffington Post*, March 1, 2010. Retrieved on May 22, 2010 from

http://www.huffingtonpost.com/marc-rotenberg/brandeis-in-italy-the-pri_b_481115.html

Rundle, M. (2007). 'e-Infrastructures for Identity Management and Data Sharing: Perspectives across the Public Sector', Oxford Internet Institute Forum Discussion Paper No. 12, University of Oxford. Available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1325235

Rundle, M. and Dopatka, A. (2009). 'Towards a Policy and Legal Framework for Identity Management: A Workshop Report'. Oxford Internet Institute Forum Discussion Paper No. 16, University of Oxford. Available at http://www.oii.ox.ac.uk/publications/FD16.pdf

Siegel, M. L. (1998). Hate Speech, Civil Rights, and the Internet: The Jurisdictional and Human Rights Nightmare. *Albany Law Journal of Science & Technology*, *9*, 375.

Silenced: Censorship and Control of the Internet. (n.d.). . Retrieved on December 31, 2009 from http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-61390&als[theme]=Silenced%20Report&headline=Silenced:%20%20Censorship%20and%20Control%20of%20the%20Internet.

Singel, R. (2009). 'Australia Censors WikiLeaks Page', *Threat Level*, 17 March. Available at http://www.wired.com/threatlevel/2009/03/australia-censo/

Sucherman, M. (2010). "Serious Threat to the web in Italy", The Official Google Blog, February 24, 2010. Retrieved on March 3, 2010 from http://googleblog.blogspot.com/2010/02/serious-threat-to-web-in-italy.html

Sutton, J. and Clarke, M. (2010). Emerging Technologies/Emerging Democracies: Information Technology, Economic Growth and Governance in Iraq. IREX. Retrieved on October 12, 2010 from http://www.irex.org/news/emerging-technologiesemerging-democracies-information-technology-economic-growth-and-governance

Tene, O. (2007). What Google Knows: Privacy and Internet Search Engines. *SSRN eLibrary*.

The Working Group on Internet Governance - WGIG (2005). Report of the Working Group on Internet Governance. Available at http://www.wgig.org/docs/WGIGREPORT.pdf

Thierer, A. D. (2007). Rep. Bean's 'Safer Net Act': An Education-Based Approach to Online Child Safety. *SSRN eLibrary*.

Thomas, K. S. R. G. D. (1998). Internet Regulation Process Model: The Effect of Societies, Communities, and Governments. *Political Communication*, *15*(4), 427. Available at doi: 10.1080/105846098198821

Travis, H. (2008). Opting Out of the Internet in the United States and the European Union: Copyright, Safe Harbors, and International Law. *Notre Dame Law Review, Vol. 83, No. 4, 2008*.

Tsesis, A. (2001). Hate in Cyberspace: Regulating Hate Speech on the Internet. *San Diego Law Review*, *Summer*.

Unintended Consequences: Ten Years Under the DMCA. Electronic Frontier Foundation (EFF), v. 5.0 (October 2008). Available at http://www.eff.org/files/DMCAUnintended10.pdf

Unwin, T. (2009) "ICTD4 Implementation: Policies and Partnerships", in *Information and Communication Technology for Development*, Tim Unwin (ed.), Cambridge: Cambridge University Press, Chapter 5.

US FCC to study ways to block sex, violence from kids | Reuters. (n.d.). Retrieved on December 31, 2009 from http://www.reuters.com/article/idUSTRE57U5T520090831

US Supreme Court (1997), Reno, Attorney General of the United States, et al. v. American Civil Liberties Union, et al., Appeal from the United States District Court for the Eastern District of Pennsylvania, No. 96-511, Argued 19 Mar., decided 26 June.

Valetk, H. A. (2009). 'Twitter Jitters: Can What You Tweet About Police Land You in Jail?', posted on Legaltech on Demand at http://www.law.com/jsp/article.jsp?id=1202434758642&Twitter_Jitters_Can_What_You_Tweet_About_Police__Land_You_in_Jail

Wafa, T. (2009). Global Internet Privacy Rights - A Pragmatic Approach. *University of San Francisco Intellectual Property Law Bulletin, Vol. 13, No. 131, 2009*.

Wagner, Ben (2009): Deep Packet Inspection and Internet Censorship: International Convergence on an 'Integrated Technology of Control. Available at http://advocacy.globalvoicesonline.org/wp-content/uploads/2009/06/deeppacketinspectionandInternet-censorship2.pdf

Wallsten, S. (2005).Regulation and Internet Use in Developing Countries. *Economic Development and Cultural Change*, *53*(2), 501-523. doi: 10.1086/425376

Waters, R. (2010), 'Online Leaks: A Digital Deluge', *Financial Times*, 30 July. Available at http://www.ft.com/cms/s/0/9098a06a-9c1c-11df-a7a4-00144feab49a.html

Watney, M. (2006). Regulation of State Surveillance of the Internet.In *ISSE 2006 — Securing Electronic Business Processes* (pp. 415-425). Retrieved on December 31, 2009 from http://dx.doi.org/10.1007/978-3-8348-9195-2_44

WGIG (2005), Working Group on Internet Governance, Report of the Working Group on Internet Governance, Château de Bossey, June. Available at http://www.wgig.org/docs/WGIGREPORT.pdf

Woodard, C. (July 1, 2003). 'Estonia, where being wired is a human right'. *The Christian Science Monitor*. Retrieved on October 10, 2010 from http://www.csmonitor.com/2003/0701/p07s01-woeu.html

Internet World Stats: Usage and Population Statistics available at: http://www.internetworldstats.com/stats.htm

Wu, T., &Yoo, C. S. (n.d.). Keeping the Internet Neutral?: Tim Wu and Christopher Yoo Debate. *Federal Communications Law Journal, Vol. 59, No. 3, 2007*.

Yang, B. (2008). NPOs in China: Some Issues Concerning Internet Communication. *Knowledge, Technology & Policy*, *21*(1), 37-42. Available at doi: 10.1007/s12130-008-9039-7

Yang, K. C. (2007). A comparative study of Internet regulatory policies in the Greater China Region: Emerging regulatory models and issues in China, Hong-Kong SAR, and Taiwan. *Telematics and Informatics*, *24*(1), 30-40. Available at doi: 10.1016/j.tele.2005.12.001

Yet another adoption of liberty killer "three strikes" law in France. La Quadrature du Net. (2009, September 21). Retrieved from http://www.laquadrature.net/en/yet-another-adoption-of-liberty-killer-three-strikes-law-in-france

Ynalvez, M. A., Duque, R. B., and Shrum, W. (2010). 'Shaping Research in Developing Areas', in Dutton and Jeffreys (2010): 325-42.

Young, J. M. (2004). Surfing While Muslim: Privacy, Freedom of Expression & the Unintended Consequences of Cybercrime Legislation. *SSRN eLibrary*.

Zittrain, J., (2003). 'Be Careful What You Ask For: Reconciling a Global Internet and Local Law', Who Rules the Net? Cato Institute, 2003. doi:10.2139/ssrn/395300. Retrieved on February 5, 2010 from http://ssrn.com/abstract=395300

Zittrain, J. (2006). 'A History of Online Gatekeeping', Harvard Journal of Law and Technology, Vol. 19, No. 2: 253. Available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=905862

Zittrain, J. and John Palfrey (2008). 'Internet Filtering', pp. 29-56 in Deibert, R., Palfrey, J., Rohozinski, R., and Zittrain, J. (eds), *Access Denied: The Practice and Policy of Global Internet Filtering*. (Cambridge, Mass: MIT Press).

Zook, M.A. (2005). *The Geography of the Internet Industry: Venture Capital, Dot-coms and Local Knowledge* (Blackwell Publishers: Oxford).

End Notes

[1] Current worldwide statistics on usage at: http://www.internetworldstats.com/stats.htm

[2] David Erdos (personal communication, 24-4-10) sees a need for a new ecology of law for the Internet to address this transfer of old media regulation to the new media of the Internet.

[3] The concept of a network society has been developed by Manuel Castells (2000, 1996), building on earlier conceptions of an information society, based on work by Daniel Bell (1974) and others.

[4] Article 19 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.' See: http://www.un.org/en/documents/udhr/

[5] See: http://news.bbc.co.uk/1/hi/world/asia-pacific/8361471.stm

[6] See: http://portal.unesco.org/ci/en/ev.php-URL_ID=2493&URL_DO=DO_TOPIC&URL_SECTION=201.html

[7] Exactly how this is realized is a matter of debate. At one extreme, this could be translated into a fundamental right for everyone on the planet to have particular technologies. Therefore, how a right to connection is translated into policy and practice is itself a major policy issue.

[8] Based on World Internet Statistics at: http://www.internetworldstats.com/stats.htm

[9] See: http://www.globalnetworkinitiative.org/principles/index.php and http://www.article19.org/pdfs/publications/1993-handbook.pdf

[10] Article 10 see: http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm

[11] See the Charter of Fundamental Rights of the European Union (2000/C 364/01) at: http://www.europarl.europa.eu/charter/default_en.htm

[12] First Amendment see: http://www.law.cornell.edu/constitution/constitution.billofrights.html

[13] African Charter on Human and Peoples' Rights see: http://www1.umn.edu/humanrts/instree/z1afchar.htm

[14] African Charter on Human and Peoples' Article 7: 'The rights and freedoms of each individual shall be exercised with due regard to the rights of others, collective security, morality and common interest.'

[15] See Decision 2009-580 DC: http://www.conseil-constitutionnel.fr/conseil-constitutionnel/english/case-law/case-law.25743.html

[16] See Costa Rican constitutional court ruling-2010-012790 (in Spanish): http://200.91.68.20/scij/busqueda/jurisprudencia/jur_repartidor.asp?param1=XYZ&param2=1&nValor1=1&nValor2=483874&strTipM=T&lResultado=1

[17] See Estonia's Public Information Act: http://unpan1.un.org/intradoc/groups/public/documents/un-dpadm/unpan039520.pdf

[18] See Article 5A.2 from the Greek Constitution: *www.nis.gr/npimages/docs/**Constitution**_EN.pdf*

[19] http://www.diputadossanluis.gov.ar/diputadosasp/paginas/NormaDetalle.asp?NormaId=779

[20] See, for example, the use of the ecology of games in studies of telecommunication policy and the development of the Internet (Dutton 1992; Dutton 2008; and Dutton et al 2008).

[21] The idea that the ARPANet was primarily focused on military and defence needs is one of the most common misconceptions surrounding the history of the Internet. See Dutton (2008).

[22] In the USA, in the late 1990s, the Department of Commerce through the National Telecommunication and Information Administration (NTIA), sponsored a Telecommunication

and Information Infrastructure Assistance Program (TIIAP). This provided matching grants to help foster the development and use new telecommunications technologies.

[23] See: http://about.skype.com/2003/08/skype_beta_launched.html

[24] Figures 1-6 are graphs created by the report authors using data drawn from Internet World Stats Usage and Population Statistics available at http://www.internetworldstats.com/

[25] See: http://www.oii.ox.ac.uk/research/project.cfm?id=46

[26] See: http://www.cpj.org/

[27] The Web Ecology Project[27] did an analysis of all the tweets about the Iranian election, such as those with the 'Iranelection' hash tag and found a standard power law distribution pattern, with 10% of individuals contributing most of the content. Tweets in Farsi were far more limited than Tweets in English, and only a minority of Tweets originated from Iran. Only 10-12 of the top 100 Twitterers originated in Iran. Most Tweets were sent by the Iranian diaspora, who were getting news in Farsi from different sources and tweeting or re-tweeting them in English.

[28] Based on extensive journalistic coverage of Vietnam, including: "Another Blogger Charged with "Subversion" faces Death Penalty". Reporters Without Borders. December 23, 2009. http://www.rsf.org/Blogger-and-activist-faces.html (Accessed on January 15, 2010); ; ; Ministry of Information and Communications of the Socialist Republic of Vietnam (MIC). http://www.mic.gov.vn/en/menu/introduction/2/index.mic (Accessed on January 16, 2010); Nga Pham. "Vietnam releases detained blogger". BBC News. September 14, 2009. http://news.bbc.co.uk/1/hi/8253832.stm (Accessed on January 16, 2010); "Vietnamese activist convicted of subversion", The Associated Press. December 28, 2009. http://www.cbc.ca/world/story/2009/12/27/activist-subversion-vietnam.html (Accessed on January 16, 2010); "Vietnam-Bloggers and writers arrested: where's freedom of expression?"Asian Forum for Human Rights and Development. September 17, 2009. http://www.forum-asia.org/index.php?option=com_content&task=view&id=2314&Itemid=32 (Accessed on January 15, 2010); "WiPC 2009 Resolution: Viet Nam". International Pen. October 2009. http://www.internationalpen.org.uk/go/committees-and-networks/writers-in-prison/wipc-2009-resolution-viet-nam (Accessed on January 16, 2010).

[29] The Communist Party of Vietnam has sought to minimize criticism about its relations with China.

[30] 10 Worst Countries to be a Blogger". Special Reports, Committee to Protect Journalists, April 30, 2009. http://cpj.org/reports/2009/04/10-worst-countries-to-be-a-blogger.php (Accessed on January 16, 2010).

[31] http://www.mic.gov.vn/en/menu/introduction/2/index.mic

[32] Amongst the eight activists sentenced, were well-known novelist and journalist Nguyen XuanNghia as well as student and Internet writer, Ngo Quynh. Earlier, three bloggers, Nguyen Ngoc NhuQuynh, Bui ThanhHieu and Pham Doan Trang were arrested for national security reasons. In December 2009, well-known human rights lawyer Le Cong Dinh, the young pro-democratic blogger Nguyen TienTrung and former army officer Tran Anh Kim were accused of "incitement of subversion" under Article 79 of the Penal Code, which carries sentences that include the death penalty. Mr. Kim was convicted to serve for five-and-a-half years in prison in December 2009. Le Cong Dinh and Nguyen TienTrung were awaiting trials in January 2010. Other well-reported cases include that of a blogger, Nguyen Van Hai (penname Dieu Cay), who received two-and-a-half years of imprisonment in 2008 for tax evasion.

[33] http://www.edri.org/issues/freedom/access

[34] This only covers countries observed by these studies. There are other countries that have been cited for strict censorship regimes, such as North Korea, the Democratic People's Republic of Korea (DPRK), by other observers, such as Reporters without Borders. See: http://en.rsf.org/web-2-0-versus-control-2-0-18-03-2010,36697

[35] A website was available that enabled users to '[t]est any website and see real-time if it's censored in China'. However, the site now notes that: 'Because of the ever stricter measures of censorship Chnia imposes on the Internet, the team … at present can no longer vouch for the reliability of its test tool.' See: http://www.greatfirewallofchina.org/

[36] Figures 7 & 8 are graphs created by the report authors using data drawn from the BBC World Service global internet poll. The original news story is available at: http://news.bbc.co.uk/1/hi/8548190.stm, and the data was drawn from the poll findings at: http://news.bbc.co.uk/1/shared/bsp/hi/pdfs/08_03_10_BBC_internet_poll.pdf . Both were accessed on 8th March 2010.

[37] http://www.iwf.org.uk/media/news.archive-2008.251.htm

[38] According to Electronic Frontiers Australia: "The Australian Federal Government has announced that it will introduce "mandatory ISP-level filtering of Refused Classification (RC) rated content." What this means is that Australian Internet Service Providers (ISPs) will now have to filter the Internet to block access to websites that would be "Refused Classification" under Australia's classification laws." (http://wiki.efa.org.au/learn_more/)

[39] P 16, http://www.aconite.com/sites/default/files/Internet_blocking_and_Democracy.pdf

[40] See: http://www.edri.org/edrigram/number7.19/draft-framework-decision-child-exploatation

[41] Reporters Without Borders: http://www.rsf.org/Prosecutors-violate-online-free.html

[42] Turkey blocked YouTube twice in 2007 and is currently blocking other websites, see: http://www.edri.org/edrigram/number7.19/turkey-blocks-foreign-websites

[43] 14 December 1946.

[44] Berlingieri (2010) argues that confusion was created around the case because the conviction relied on the combination of two articles that were considered related as a 'matter of fact' by the judge. According to Berlingieri, it is unclear why Section 13 was used since it was not mentioned in the indictment. (Section 13 is found in Section 161, and not 167 of the code). Charges related to infringement of privacy and "unlawful processing of data" should be based on Section 167, a section that does not include the use of 'prior notice'.

[45] See the Pirate Bay trial, which was a joint criminal and civil prosecution in Sweden of four individuals charged for promoting the copyright infringement of others with The Pirate Bay site. The accused were all found guilty and sentenced to serve one year in prison and pay a fine of 30 million Swedish krona (app. €2.7 million or USD 3.5 million). http://en.wikipedia.org/wiki/Pirate_bay

[46] Deibert et al (2008).

[47] OpenNetInitiative: Asia http://opennet.net/research/regions/asia

[48] See 47 U.S.C. § 230(c)(1). (http://www.techlawjournal.com/courts/zeran/47usc230.htm)

[49] See Google's principles or philosophy at: http://www.google.com/corporate/tenthings.html

[50] http://www.google.com/governmentrequests/

[51] http://googleblog.blogspot.com/2006/02/testimony-internet-in-china.html

[52] http://googleblog.blogspot.com/2010/01/new-approach-to-china.html

[53] Rebecca MacKinnon, ex-foreign correspondent in China for CNN and current fellow at the Open Society Institute, said that while working in China, Google.cn tended to present search results that were less filtered than its Chinese competitor Baidu (Mackinnon 2010).

[54] As reported by many business and political experts, Google has more interest in preserving its markets outside rather than in China, where it is only the second most popular search engine after Baidu, but holds only a third of the Chinese market share (Anderson 2010).

[55] http://www.state.gov/secretary/rm/2010/01/135519.htm

[56] http://english.people.com.cn/90001/90780/91344/6873383.html

[57] http://googleblog.blogspot.com/2010/03/new-approach-to-china-update.html

[58] http://googleblog.blogspot.com/2010/03/new-approach-to-china-update.html

[59] For example, RIM shares fell on July 27th and 28th, 2010, when the UAE threatened a shutdown, and rose on August 10th, 2010 when RIM announced they would be moving servers into Saudi Arabia to provide a technical monitoring solution.

[60] In 1994, FBI Director, Louis Freeh, responded to a question in a press conference by saying that if Clipper failed to gain public support, and FBI wiretaps were shut out by non-government-controlled cryptography, his office would have no choice but to seek legislative relief. Later, in the aftermath of the Oklahoma City tragedy, Mr. Freeh testified before the Senate Judiciary Committee that public availability of strong cryptography must be curtailed by the government. See: http://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html.

[61] See: http://security.homeoffice.gov.uk/ripa/interception/

[62] The European Directive 2006/24/EC on 'the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks' requires member states to make sure their communications providers retain, for a period of between 6 months and 2 years, data that helps identifying the source of a communication, the destination of a communication, the date, time and duration of a communication, the type of communication, the communication device, and the location of mobile communication equipment 'for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law'. See Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF

[63] The OII has held two workshops around identity management, including those reported by Rundle (2007) and Rundle and Dopatka (2009).

[64] For example, this debate arose in the deliberations of RISEPTIS (2009), but also in a committee focused on privacy and data protection (RAE 2007).

[65] Reported by BBC News, 24 July 2010. See: http://www.bbc.co.uk/news/uk-10750077