REFERENCE SERIES NO. 6

MAPPING DIGITAL MEDIA:
FREEDOM OF EXPRESSION RIGHTS IN THE DIGITAL AGE

By Andrew Puddephatt

OPEN SOCIETY
FOUNDATIONS

April 2011

Freedom of Expression Rights in the Digital Age

WRITTEN BY

Andrew Puddephatt[1]

This paper assesses the impact of digital communications on the right to freedom of expression. Specifically, it examines the internet and world wide web as a new platform for freedom of expression, one that encourages peer-to-peer collaboration as well as traditional one-to-many forms of communication.

The paper also considers the jurisdictional vacuum created by the web and internet and the techniques developed to deal with this vacuum, with a focus on intermediaries such as internet service providers.

Finally, it looks at new tools to promote freedom of expression, and new threats to it, including a kind of privatised censorship emerging on the internet. New forms of human rights activism need to be developed with a range of international bodies, defining normative standards on how free expression should be protected online. At the same time, dialogue and co-operation on these issues should be fostered with digital communication companies.

[1] Andrew Puddephatt is a director of Global Partners & Associates, in London.

Mapping Digital Media

The values that underpin good journalism, the need of citizens for reliable and abundant information, and the importance of such information for a healthy society and a robust democracy: these are perennial, and provide compass-bearings for anyone trying to make sense of current changes across the media landscape.

The standards in the profession are in the process of being set. Most of the effects on journalism imposed by new technology are shaped in the most developed societies, but these changes are equally influencing the media in less developed societies.

The Media Program of the Open Society Foundations has seen how changes and continuity affect the media in different places, redefining the way they can operate sustainably while staying true to values of pluralism and diversity, transparency and accountability, editorial independence, freedom of expression and information, public service, and high professional standards.

The **Mapping Digital Media** project, which examines these changes in-depth, aims to build bridges between researchers and policy-makers, activists, academics and standard-setters across the world.

The project assesses, in the light of these values, the global opportunities and risks that are created for media by the following developments:

- the switchover from analog broadcasting to digital broadcasting
- growth of new media platforms as sources of news
- convergence of traditional broadcasting with telecommunications.

As part of this endeavour, Open Society Media Program has commissioned introductory papers on a range of issues, topics, policies and technologies that are important for understanding these processes. Each paper in the **Reference Series** is authored by a recognised expert, academic or experienced activist, and is written with as little jargon as the subject permits.

The reference series accompanies reports into the impact of digitization in 60 countries across the world. Produced by local researchers and partner organizations in each country, these reports examine how these changes affect the core democratic service that any media system should provide—news about political, economic and social affairs. Cumulatively, these reports will provide a much-needed resource on the democratic role of digital media.

The **Mapping Digital Media** project builds policy capacity in countries where this is less developed, encouraging stakeholders to participate and influence change. At the same time, this research creates a knowledge base, laying foundations for advocacy work, building capacity and enhancing debate.

The **Mapping Digital Media** is a project of the Open Society Media Program, in collaboration with the Open Society Information Program.

MAPPING DIGITAL MEDIA EDITORS

Marius Dragomir and Mark Thompson (Open Society Media Program).

EDITORIAL COMMISSION

Yuen-Ying Chan, Christian S. Nissen, Dušan Reljić, Russell Southwood, Michael Starks, Damian Tambini.

The Editorial Commission is an advisory body. Its members are not responsible for the information or assessments contained in the Mapping Digital Media texts.

OPEN SOCIETY MEDIA PROGRAM TEAM

Biljana Tatomir, deputy director; Meijinder Kaur, program assistant; Morris Lipson, senior legal advisor; Miguel Castro, special projects manager; and Gordana Jankovic, director

OPEN SOCIETY INFORMATION PROGRAM TEAM

Vera Franz, senior program manager; Darius Cuplinskas, director

The views expressed in this publication do not represent, or necessarily reflect, the views of the Open Society Foundations.

Contents

I. Introduction

Freedom of expression has long been regarded as a fundamental right, which is important in itself and also helps to defend other rights and freedoms. If it is to be fully realized, however, freedom of expression requires a public dimension—a means of communication—in order to facilitate the exchange of opinions, ideas and information. It follows that free expression activists have focused a great deal of attention on the structure and regulation of the media environment, for it is these that provide the principal platforms for public expression, from books and newspapers to the broadcast media.

Much attention has been paid to the norms and principles that freedom of expression requires in the traditional media world. The consensus is that a media environment supporting free expression will have a number of characteristics: a diverse media environment, part public, part private and part community; a plurality of different media outlets; and a system that is broadly self-regulating with the exception of broadcast media (where spectrum has been limited and a regulatory body allocates bandwidth).

Where restrictions upon freedom of expression are regarded as necessary, they have been carefully defined in international human rights laws covering issues such as defamation, incitement to violence and hate speech. These restrictions are to be enforced through national or international courts.[2] While digital communications do not change these basic principles in any fundamental way, they do require recognition that there are new forms of censorship, new questions of jurisdiction, and new norms and standards to develop.

[2] Examples have been accumulated by Article 19 at http://www.article19.org/publications/law/standard-setting.html or UNESCO's Guide to Broadcast Regulation http://unesdoc.unesco.org/images/0018/001832/183285e.pdf (accessed 22 November 2010).

II. What Are Communications in the Digital Age?

The communications environment has been transformed by the ability to turn different kinds of information, whether voice, sound, image or text into digital code, accessible by a range of devices from the personal computer to the mobile phone. The emergence of the internet has transformed communication capacity from something essentially local (be it a locality or a country) into a medium that is truly global. The creation of the world wide web,[3] a service that operates over the internet, was the means to make enormous volumes of content available. It did so by providing three key functions: a publishing format, HyperText Markup Language (HTML); an address for each piece of information (known as its Uniform Resource Locator or URL); and a means of transferring information, through the HyperText Transfer Protocol (http). Finally, the creation of an electronic mail system based on a "store and forward" model provided by intermediaries has allowed e-mail to emerge as probably the dominant form of "one to one" communication globally.

It is this combination of networks and services operating globally that creates so many communication possibilities in the digital world. It has created new space for publication, with virtually no entry costs (unlike the traditional offline media). It allows peer-to-peer collaboration in the form of user-generated and user-mediated content. In this sense, it has the capacity to lead to what we might call the "democratization" of freedom of expression in the public realm. Previously, an elite group—formed by journalists, publishers, media owners, even government censors—determined who wrote for a public. The growth of the internet and the web bypasses these gatekeepers and allows anyone to be a writer, broadcaster or publisher. The facility to provide and access material seems to offer almost limitless possibilities for producing, sharing and exchanging content of all kinds.

[3] See http://www.w3.org/ for background (accessed 22 November 2010).

In their first incarnation, the internet and web were hailed as offering a new global, boundless space able to evade traditional censorship. John Gilmore, a libertarian activist and founder of the Electronic Frontier Foundation (whose name suggests its perspective), was quoted in *Time* magazine as saying "The Net interprets censorship as damage and routes around it."[4]

Today, of course, the net has become a more contested, enclosed and nationalized space, but both the libertarian possibilities and the new forms of domination and control have recast the challenge to freedom of expression in the modern era.

[4] First quoted by Philip Elmer-DeWit, "First Nation in Cyberspace", *Time* Magazine, 6 December 1993.

III. A Universal Jurisdiction?

What are the characteristics of this space that impact upon free expression rights? As a network of networks, the internet is an international platform which has no overarching jurisdiction. No single entity governs the totality of the internet: governance is provided by different components and institutions operating in very different jurisdictions. A program can be made in the Ukraine, uploaded onto a U.S. server, and downloaded in Ghana.

The international jurisdictional bodies such as the Internet Corporation for Assigned Names and Numbers (ICANN),[5] the International Telecommunication Union (ITU), and the World Wide Web Consortium (W3C),[6] like the national bodies which administer the national domains, are concerned with the efficient working of the system, its *functionality*, rather than governing the environment in the way that regulators govern broadcast media.

Consequently, there is a jurisdictional vacuum over content on the web. If there is a need to restrict freedom of expression in accordance with the carefully developed norms applied to the traditional media, it is not clear how such authority should be appropriately applied given that there is no means of regulating content internationally, nor any consensus on the norms that need to be applied. The resulting vacuum of authority has been filled by frequently arbitrary actions with a number of adverse consequences. A recent proposal to establish an inter-governmental policy forum for the internet has been suggested by India, Brazil and South Africa, though some are concerned that no civil society voices would be admitted to its deliberations.[7]

[5] See http://www.icann.org/ ICANN was founded in 1998.

[6] See http://www.w3.org/ Founded in 1994, W3C is administered by a consortium of research institutions and universities.

[7] See http://unpan1.un.org/intradoc/groups/public/documents/un-dpadm/unpan043559.pdf.

IV. Policy Concerns

In 2000, a French court ruled that Yahoo! had to block French internet users from accessing a Nazi memorabilia site based in the United States. After contemplating the technical problems, Yahoo! removed the site completely even though it was legal in other jurisdictions. Whatever one's view of the merits of the case, in this instance a French standard on free expression was effectively exported to the rest of the world.[8] Companies such as Facebook have come under intense political pressure to remove material that is deemed offensive but remains legal, as they did over a recent case involving Sarah Palin.[9]

In effect we are seeing the emergence of a privatized form of censorship, applied across a range of issues, from alleged intellectual property violations, to a range of defamation issues. Child pornography provides a stark illustration of the problem. There is little doubt that the internet has facilitated the exchange of contacts among those who abuse children, or that there is a significant international traffic in child sex images. In some countries, private organizations have been established—such as the UK's Internet Watch Foundation (IWF)—which are largely funded by the communications industry.[10] The IWF supplies a list of internet sites and content that are potentially illegal to internet service providers, most of which then take down or block the sites on a voluntary basis. There is no transparency about the sites identified, no legal redress (as this is a form of self-censorship by ISPs), and no independent legal scrutiny.[11] No one would argue that child pornography should be available online, but there is a concern about "due process" when a form of privatized censorship is introduced and operated by an industry-funded charity.

Instances like this are increasing. Internet service providers (ISPs), which traditionally expected to be mere conduits for the services they carry, are being asked to collect data on their users (for example, by the EU Data Retention Directive 2006/24/EC) and even to monitor browsing histories through voluntary agreements with governments that have no legal scrutiny.[12] Where providers of content then merge with carriers of content—for example with Virgin Media in the UK—the pressure to collect even more data on users becomes intense.

[8] An analysis of the case by Yaman Akdeniz is available at http://www.cyber-rights.org/documents/yahoo_ya.pdf (accessed 22 November 2010).

[9] Joe MacNamee, *The Slide from "Self regulation" to Corporate Censorship,* Brussels: European Digital Rights (EDRi), 2010.

[10] See http://www.iwf.org.uk/ (accessed 22 November 2010).

[11] Frank Fisher, "A nasty sting in the censors' tail", the *Guardian,* 9 December 2008. Available at http://www.guardian.co.uk/commentisfree/2008/dec/09/scorpions-virgin-killer-censorship (accessed 14 November 2010).

[12] McNamee.

Virgin have announced that they intend to undertake deep packet inspection of 40 percent of its customers in order to counter violations of its intellectual property rights, but such a data pool will prove irresistible to governments in the future.

Moreover, blocking is inaccurate and ineffective. As even the IWF acknowledges, illegal sites move quickly and are increasingly using hacked servers to carry their content. Richard Clayton even argues that some blocking mechanisms can be used to locate child abuse material, turning a system designed to block it into one that can facilitate it.[13] When democratic states undertake such blocking, they indicate that this is an acceptable way of controlling content and provides a market for censorship technologies. Some of the countries most hostile to free expression have spoken about implementing pervasive blocking systems, supposedly to fight pornography or "harmful content," as in the widely quoted example of China's Green Dam,[14] often exploiting technologies developed in democratic countries. For example, Iran relies on commercial software (SmartFilter, made by the U.S.-based company, Secure Computing) to implement its web-filtering processes and focuses on feminist sites because of their alleged pornographic content.[15]

Another way of undermining freedom of expression is to make intermediary institutions liable for the content they carry. Intermediary institutions—given the 'network of networks' structure of the internet—are crucial to its effective performance. There is a vast range of intermediaries from internet service providers themselves, through website hosting companies, companies that provide video and photo sites like YouTube and Flickr to others which provide blog platforms, e-mail and social networking such as Facebook. These are all essential if the digital world is to facilitate freedom of expression, allowing individuals to share information and ideas directly with each other over the internet.

While it is obvious that those who create illegal content should be liable under civil or criminal law, prosecuting those who simply carry or host that content has a significant chilling effect upon free expression as it makes every intermediary wary of carrying material that may be subject to prosecution in one jurisdiction or another. Given how much content is available on the web, governments have become nervous and keen to introduce controls. Sometimes these are direct; the UK Digital Economy Act requires ISPs to collect personal data, block online resources, or co-operate with sanctions. In other instances, the lack of overt legal guidance and understandable wariness about carrying controversial material leads to over-zealous actions by ISPs and a willingness to take down controversial material simply if someone complains.[16] This results in what is, in effect, a broad regime of censorship that contrasts with the narrow interpretations of the law and careful application of standards expected in the offline world.

Some have argued that a universal regulatory framework might facilitate a common approach to free expression. But experience with the Council of Europe's Cybercrime Convention shows that reconciling the contrasting provisions of different domestic legal systems into one international standard would risk lowering

[13] Richard Clayton, "Failures in a Hybrid Content Blocking System", in *Privacy Enhancing Technologies*, 2005, pp. 78–92, available at http://www.cl.cam.ac.uk/~rnc1/cleanfeed.pdf (accessed 20 November 2010).

[14] See http://news.bbc.co.uk/1/hi/world/asia-pacific/8091044.stm.

[15] See http://www.isiswomen.org (accessed 20 November 2010).

[16] McNamee.

the free expression protections that are implicit in a more open, unregulated system.[17] In particular, the treaty lacks a "dual criminality" provision where an offence is required to have been committed in both jurisdictions before action can be taken. This opens the door to the authorities of a more open jurisdiction co-operating in pursuit of an action that is perfectly legal in their own territory. In a world of vastly varying standards, a common approach could drive global standards down.

Pressure from law enforcement agencies for greater controls, combined with a lack of legal protections for freedom of expression online, are creating a situation where decisions about what and what not to host are frequently taken by private companies—and often by local staff in those companies that are subject to enormous pressure by host governments. Microsoft in Russia recently came under pressure to provide access to communication by dissidents on the bogus grounds of alleged software privacy and only resisted once the U.S. media began to take an interest in the case. This echoes the case of Yahoo! in China, which accepted that it was obliged by Chinese law to identify two Chinese journalists using the internet, who were subsequently sentenced to ten years in prison.[18] In neither case were free expression considerations a factor in the company's response.

It is easy to berate companies that fail to protect rights to free expression in this way. But if we leave companies to be the standard bearers for free expression rights, we need to explain what those standards mean and how they can be applied. One initiative that aims to provide this support—and monitoring of corporate behavior—is the Global Network Initiative (GNI), a partnership between communication companies and human rights groups that provides guidelines on how companies can operate in challenging political environments and monitors corporate compliance.[19] Governments should also be much more explicit that they seek to defend free expression rights on the internet and not just discuss the internet as a threat to security. In turn, civil society organisations need to engage with communications companies to help—or pressurize—them into adopting free expression principles in the way they do business.

Building upon these kinds of steps, there is a need to develop normative standards that promote freedom of expression and which can be used to shape policy and regulation at the national and international level through mechanisms like the Internet Governance Forum (IGF), a multi-stakeholder forum for governments, business and civil society established by the United Nations to promote discussion of internet policy.

It is important to make sure that a strong free expression standard is promoted in more commercial forums like the OECD, the WTO and WIPO,[20] where internet policy issues are considered. It is also important to encourage bodies traditionally concerned with human rights, such as the United Nations, the Council of Europe, the Inter-American and African Commissions on human rights, to be aware of the issues raised by digital communications. If the new initiative sponsored by Indian, South Africa and Brazil (see *section 3*) succeeds, it will very likely have the effect of marginalizing ICANN and the IGF process.

[17] The Cybercrime Convention text is available at http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm. A critique by the Electronic Privacy Information Center is available at http://epic.org/privacy/intl/ccc.html (accessed 15 November 2010).

[18] "Microsoft and Russia", the *New York Times*, 14 September 2010, available at http://www.nytimes.com/2010/09/15/opinion/15wed2.html (accessed 15 November 2010).

[19] See http://www.globalnetworkinitiative.org/ (accessed 15 November 2010).

[20] Organization for Economic Development, at http://www.oecd.org; World Trade Organization, at http://www.wto.org/; World Intellectual Property Organization, at http://www.wipo.in (accessed 15 November 2010).

V. New Tools and Dangers

Alongside the need to promote free expression policies, free expression activists should be aware of the new tools available online to both to promote freedom of expression, and also the new tools for censorship embedded in digital technologies.

On the upside, the tools that help human rights activities evade censorship and control are multiplying. Mobile phones can stream police brutality directly to the web in Burma; digital cameras record ill treatment in Abu Ghraib; text messaging can mobilize millions and topple presidents as it did in the Philippines; Farsi websites can provide the medium for Persian poetry and Iranian politics that is denied in conventional space; circumvention technologies such as the use of proxy servers can help to get around censorship.

But there are also dangers. The very technologies that allow us to connect with each other—can also be used to track those protestors down as happened with Nokia Siemens Networks phone technology during the elections in Iran.[21]

New forms of censorship can be built into the very software and hardware that makes up the internet. The most glaring example of this was the Chinese government's attempt in 2009 to insist that software known as Green Dam be built into all personal computers sold in China.[22] China has more internet and mobile phone users than anywhere else, and the Chinese authorities have imposed the most extensive systems of censorship in the world.[23] As well as filtering content using routers and servers, there is evidence that they utilize the "store and forward" function of intermediaries to hold material such as blogs in a queue indefinitely.[24]

[21] See http://www.techeye.net/business/nokia-siemens-hinder-iranian-human-rights-says-nobel-winner (accessed 15 November 2010).

[22] This software monitors individual computer behavior by installing components in the operating system and would have given the authorities direct power to control access to content (as well as allowing remote control of the computer running the software). The proposal was finally defeated through the WTO on trade grounds. See http://opennet.net/chinas-green-dam-the-implications-government-control-encroaching-home-pc and http://www.cse.umich.edu/~jhalderm/pub/gd/ (accessed 15 November 2010).

[23] See http://opennet.net/research/profiles/china (accessed 15 November 2010).

[24] See http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2378/2089 (accessed 15 November 2010).

In 2006, the Ministry of Public Security announced the launch of the "Golden Shield" project, designed to become a national system of a digital surveillance. Along with extensive legal controls on content and a party-organized network of over 250,000 web commentators who support the regime, there are formidable pressures to exercise self-censorship.[25]

A significant weapon in the hands of such regimes is the denial-of-service (DoS) attack. In this case a target website is saturated with requests for information until it cannot respond to its regular traffic, or responds so slowly that it effectively ceases to function. Most notoriously, this appears to have been used by Russian criminals against Georgian sites during the conflict in 2008,[26] but there are many other instances, particularly directed against the websites of exiled groups such as those of the Burmese opposition.[27] To defend against these attacks requires the specialist support of technical companies and most rights-based NGOs are simply not equipped to withstand the pressure.

Finally a new threat to free expression is emerging in countries where governments are removing whole application platforms, as happened with YouTube in Turkey or the attempts to ban Facebook in Pakistan. In these cases, applications are either banned outright or—as with Research in Motion's BlackBerry e-mail service in India—only allowed to operate if traffic is routed through local servers that are easy to intercept. The overall impact is to close down the potential for freedom of expression.

One further important aspect of censorship of the internet is the evolving nature of the techniques employed. As repressive states mobilize their resources, there is a real danger that censorship will change from becoming something that is overt and technical, like the 'Great Firewall' of China, to something more complex or normative, using techniques such as DoS attacks, targeted malware, increased surveillance of users and at key points of the internet's infrastructure, applying for take-down notices based on voluntary agreements with companies (outsourcing controls to private parties), and legally binding terms-of-use agreements.

These developments reflect what many see as a growing colonization of cyberspace by states. Moreover, in many cases the techniques used by repressive states were originally developed by democratic governments in ill-thought out attempts to curb the libertarian nature of the online world.[28] Censorship and control of the internet by governments has become more obvious and pervasive and is rapidly becoming a global norm, not just a characteristic of repressive governments. As the liberating power of internet communications becomes more apparent, and forms of access to content become more mobile and flexible—such as the smart phone—and as content becomes available in a wider range of local languages, not just English, the imperative to

[25] See http://opennet.net/research/profiles/china (accessed 15 November 2010) and http://www.access-controlled.net/ (accessed 21 December 2010).

[26] See http://www.computerworld.com/s/article/9112443/Russian_hacker_militia_mobilizes_to_attack_Georgia (accessed 15 November 2010).

[27] See http://www.i-m-s.dk/article/stop-cyber-attacks-against-independent-burmese-media (accessed 15 November 2010).

[28] For extensive discussion of this development, see OpenNet Initiative, *Access Controlled: the Shaping of Power, Rights and Rule in Cyberspace*, Cambridge, MA: MIT Press, 2010.

control this new source of free expression becomes more challenging. A new and frightening possibility has emerged: that

> early commentators were correct about the magnitude of the impact of the Internet on democracy—they just got the direction wrong. Could authoritarian regimes, and also democratic governments working with private companies, be perfecting a new form of authoritarianism, working with the grain of Internet communication and exploiting the intimate entwining of online communication with the everyday lives of citizens?[29]

[29] Sahar, "Caught in the Net: "Science" book review of Access Controlled," 1 October 2010, available at http://www.access-controlled.net/2010/10/ (accessed 16 December 2010).

VI. What Is to Be Done?

Neither the possibility that the internet can democratize freedom of expression, nor the potential for a new form of authoritarianism should be underestimated, but at the moment no single direction is certain. It is vital that free expression activists are aware of the new threats, and respond to them. Defending freedom of expression online has become a vital task for the modern human rights movement. It means learning new skills and developing new capacities to fight censorship in the digital world. To help, there is a new generation of internet savvy organizations—*MobileActive*, *AccessNow*, International Media Support's *Media Frontiers*, to name but three—capable of forming new partnerships and alliances.[30] There is also a large community of technologists happy to support human rights activity. But alliances between the technologists and the human rights world will need to be actively forged, in order to encourage the development of new innovative tools that promote human rights, and to ensure that a new generation of activists is competent and equipped to tackle new kinds of digital censorship.

Globally there are continuing attempts to bring the internet under government control. The internet began as a set of interconnected U.S. military computers and developed into a research network connecting academic institutions. Today it is a public communications utility, whose infrastructure is essential to a country's security, economic, planning, health and education needs, indeed all the services that governments provide and businesses need. However, while it might be considered a public utility it is still fuelled by private sector investment and its capacity (unlike any public utility) is expanding by several times its own volume year-on-year, requiring the injection of vast amounts of capital. In recent years it has become the subject of increased attention by states which are beginning to see cyberspace as yet another forum for geopolitical competition.[31]

Responding to the politicization and colonization of the internet with a round of global regulation would be inimical to the creative drive of the competitive markets that created the internet and associated services in the first place. Moreover, any new global regulatory framework is likely to be hostile to freedom of expression in the current political climate. In these circumstances, how is international public policy to be made about the digital communications environment?

[30] For MobileActive, see http://mobileactive.org/; for Accessnow, see https://www.accessnow.org/; for Media Frontiers, see http://www.media-frontiers.org/About/GovernanceofMediaFrontiers/tabid/136/Default.aspx (accessed 16 December 2010).

[31] The United States inaugurated United States Cyber Command (USCYBERCOM) as part of its overall strategic operations in May 2010.

Firstly, users should be encouraged to care about human rights, by grasping that the online freedom which they enjoy (where they can enjoy it) is something perishable that has to be actively defended. It is crucial to bring together civil society constituencies across the fields of human rights, democracy, technology groups and communication activists, as well as reaching across sectors to include government and business. Above all, we have to re-imagine what the human right to freedom of expression means in the digital world and grasp the possibilities that the new communications environment offers us.

Secondly, there is the need to develop normative standards that can be applied across various international forums. One locus is the Internet Governance Forum where the dialogue that it permits is an important element in creating the basis for new free expression norms by securing buy-in from multi-stakeholder collaboration between government, business and civil society, and which can feed into other bodies such as ICANN where there is a series of discussions relevant to freedom of expression. But other forums such as the OECD, WTO and WIPO mentioned above are also crucial. The IGF is a multi-stakeholder forum and civil society groups are entitled to attend and debate policy issues. What is lacking first and foremost in these forums is a clear understanding of how technical, regulatory or market-driven changes in the internet can have implications for free expression. The immediate priority is to make sure that all participants at all policy forums understand how free expression principles underpin the development of the internet.

Finally, there's a need for more active partnership and dialogue with companies, including technology, media, software, and hardware companies. There is a potential alignment of companies' business interests with human rights values in different policy areas. The internet and associated applications grew from a business climate marked by innovation and openness, and innovation can help deliver economic growth and address a range of social and environmental policy goals. A competitive communications environment with minimum regulatory controls will be one where free expression principles can flourish notwithstanding individual companies' desire to monopolize business. We can establish forums to bring together free expression and human rights groups with key communications companies (applications and telecoms) to promote human rights values. The Aspen Institute in Washington, D.C. has begun an international collaboration along these lines;[32] others are likely to follow.

Above all, there is a need to understand both the opportunities and dangers of the present moment. The assumption that the internet would be a new free universe outside conventional constraints now looks sadly optimistic. What was once an electronic open frontier is now a heavily contested geo-politically shaped space where governments and companies create barriers to the free flow of information and ideas. Free expression activists should work to keep the space open through innovative policy work, by thinking how to apply free expression principles and values in the digital world, becoming expert users of the tools that are available, and actively building contacts with allies on the technological front.

[32] The Aspen Institute IDEA Project aims to identify ways to foster the freedom to connect; preserve open, end-to-end networks; and facilitate the free flow of communications across borders in a unified internet. See http://www.aspeninstitute.org/policy-work/communications-society/programs-topic/global-projects/idea (accessed 19 December 2010).

Further Reading

BBC News, *Internet Access is a "Fundamental Right"*, 8 March 2010, available at http://news.bbc.co.uk/1/hi/8548190.stm.

Benkler, Y. *The Wealth of Networks.* Yale University Press, 2006. Available at http://www.benkler.org/Pub.html

Brown, I. "Internet Self-Regulation and Fundamental Rights" (January 21, 2010), *Index on Censorship*, March 2010. Available at SSRN: http://ssrn.com/abstract=1539942

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

Center for Democracy and Technology, *Intermediary Liability 2010,* available at http://cdt.org/paper/intermediary-liability-protecting-internet-platforms-expression-and-innovation

Deibert, R., Palfrey, J., Rohozinski, R., and Zittrain, J. eds, *Access Denied: The Practice and Policy of Global Internet Filtering.* Cambridge, MA: MIT Press. Available at http://opennet.net/accessdenied

Drake, W. Jorgensen, R. "Introduction". In R. Jorgensen ed., *Human Rights in the Global Information Society.* Cambridge, MA: MIT Press, 2006.

Horner, L. *Shaping the Networked World: Drivers of Change in the Networked Communications Environment.* Paper of the Freedom of Expression Project, 2007, available at http://www.freedomofexpression.org.uk/resources/shaping+the+networked+world

Goldmith J. and Wu, T. *Who Controls the Internet? Illusions of a Borderless World.* Oxford: Oxford University Press, 2006.

Global Network Initiative, *Protecting and Advancing Freedom of Expression and Privacy in Information and Communications Technologies.* Written statement for State Judiciary Subcommittee on Human Rights and the Law, 2 March 2010.

ITU, *Measuring the Information Society, 2010*, Executive Summary, available at http://www.itu.int/ITU-D/ict/publications/idi/2010/index.html

Internet World Statistics, *Internet Growth Statistics: Today's Road to e-Commerce and Global Trade,* 9 April 2010, available at http://www.internetworldstats.com/emarketing.htm

Lessig, L. *The Future of Ideas: The Fate of the Commons in a Connected World.* New York: Random House, 2001.

MacKinnon, R. *China's Censorship 2.0: How Companies Censor Bloggers.* 2 September 2009, available at http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2378/2089

OpenNet Initiative (ONI), *China Briefing,* 15 June 2009, available at http://opennet.net/research/profiles/china

ONI, *About Filtering,* available at http://opennet.net/about-filtering

ONI, *Global Internet Filtering Map,* available at http://map.opennet.net/filtering-pol.html

ONI, *Access Controlled: the Shaping of Power, Rights, and Rule in Cyberspace.* Cambridge, MA: MIT Press, 2010.

Sen, A. *Development as Freedom.* Oxford: Oxford University Press, 1999.

Vitaliev, D. "Content and Censorship". In *APC ICT Policy Handbook,* November 2009, available at http://www.apc.org/en/pubs/books/apc-ict-policy-handbook-second-edition

Mapping Digital Media is a project of the **Open Society Media Program** and the **Open Society Information Program.**

Open Society Media Program

The Media Program works globally to support independent and professional media as crucial players for informing citizens and allowing for their democratic participation in debate. The program provides operational and developmental support to independent media outlets and networks around the world, proposes engaging media policies, and engages in efforts towards improving media laws and creating an enabling legal environment for good, brave and enterprising journalism to flourish. In order to promote transparency and accountability, and tackle issues of organized crime and corruption the Program also fosters quality investigative journalism.

Open Society Information Program

The Open Society Information Program works to increase public access to knowledge, facilitate civil society communication, and protect civil liberties and the freedom to communicate in the digital environment. The Program pays particular attention to the information needs of disadvantaged groups and people in less developed parts of the world. The Program also uses new tools and techniques to empower civil society groups in their various international, national, and local efforts to promote open society.

Open Society Foundations

The Open Society Foundations work to build vibrant and tolerant democracies whose governments are accountable to their citizens. Working with local communities in more than 70 countries, the Open Society Foundations support justice and human rights, freedom of expression, and access to public health and education.

For more information:

Open Society Media Program
Open Society Foundation

4th Floor Cambridge House, 100 Cambridge Grove
London, W6 0LE, United Kingdom

mappingdigitalmedia@osf-eu.org
www.mappingdigitalmedia.org
www.soros.org/initiatives/media

Cover Design: Ahlgrim Design Group
Design and Layout: Judit Kovács l Createch Ltd.

OPEN SOCIETY
FOUNDATIONS