Future Challenges of the Information Society

Mogens Schmidt and Sylvie Coudray

Future Challenges to Building Knowledge Societies

Introduction. The transformation in the nature and development of human knowledge is one of the most pervasive changes in the last century and is largely responsible for the compression of space and time experienced by greater numbers of people.

UNESCO encourages the construction of "Knowledge Societies", which goes beyond the narrower concept of the "Information Society" by recognizing the multilayered strands of knowledge that contribute to the making of the world. The concept of the Knowledge Society encourages the growth of capacity building so that information can be identified, produced, processed, transformed, disseminated and used as knowledge for human and social development.

Information, communication and knowledge are at the core of human progress, endeavour and well-being. Along with the Knowledge Society comes the concomitant recognition that all societies are innovative in the face of challenges and can contribute to the flow of knowledge in the world. Indeed, the concept offers a holistic and comprehensive vision with a clear development-oriented perspective that captures the complexity and dynamism of current changes in the world.

Current Challenges to Building Knowledge Societies for All. Traditional and new information and communication technologies (ICT) open up completely new opportunities to attain

higher levels of development for the benefit of millions of people in all parts of the world. In light of these technological advances and their pervasive societal and ethical implications and impacts, UNESCO's mandate to "promote the free flow of ideas by word and image" and to "maintain, increase and spread knowledge", takes on new dimensions. It exerts an even greater responsibility on the Organization to contribute proactively to addressing potential challenges, maximizing benefits and supporting equitable access to the opportunities provided by ICT to all people. The most serious of these challenges are not technological but social and they force us to answer the most fundamental questions at the heart of the development today. These challenges include the issue of freedom of expression, the goal of education for all, universal access to knowledge and information, and cultural and linguistic diversity. What they have in common is the call to continuously adapt and affirm our commitment to free flow of information as a fundamental principle underlying the production and exchange of knowledge in society.

The concept of knowledge societies acknowledges the inequalities in access to the conditions of production and reception of knowledge on a world scale, especially in terms of access to new information technologies (ICT). New information technologies offer lightning-fast access to the world's body of knowledge and the possibility of instant exchange of perspectives and information for many people on the globe. Nevertheless, the "digital divide" is a stark reality, with 80 per cent of the world's population lacking access to basic telecommunications, approximately 860 million illiterates and 2 billion people lacking electricity. But the real issues in the creation of knowledge societies are less technological than human – how can we take the human dimension into account when dealing with the "digital divide" and why is it important?

Principles for Building Inclusive Knowledge Societies. From its mandate to encourage free flow, UNESCO has identified four key principles at the heart of its work in developing knowledge societies:

The **first**, the principle of freedom of expression, must apply not only to traditional media but also to new media, including the Internet. It is the basic premise of knowledge societies. UNESCO, whose mandate is to promote the "free flow of ideas by word and image", is therefore acting unequivocally in keeping with Article 19 of the Universal Declaration of Human Rights.[1] It is important then to continue to mobilize energies and efforts to promote freedom of expression and its corollary, freedom of the press, as a basic right indispensable to the exercise of democracy. Freedom of expression is a major avenue through which creativity, innovation, criticism and questioning can be brought. This has enabled citizens to gather information and mobilize coalitions in major policy debates, and to trigger improvements in government efficiency and transparency through better communication with citizens. Our insistence on the plural form of knowledge societies rests on the conviction that there is no single uniform model, dictated by technology or market relations, to which all societies must conform. The nature of knowledge societies should be conceived as plural, variable and open to choice, and freedom of expression is inseparable from this vision.

The **second principle**, access to quality education for all, is essential for building and developing the necessary skills and capacities for development, progress and social peace in all societies. This is a fundamental right, confirmed in Article 26 of

1 Article 19 of the Universal Declaration of Human Rights: "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."

the Universal Declaration[2], as well as a tool for combating illiteracy, marginalization, poverty and exclusion. Education is the greatest capacity-builder of all. Without education, knowledge societies cannot exist. As knowledge becomes central to development, the worldwide challenge of providing quality lifelong educational opportunities for all is becoming critical. Throughout history, education has been constrained within an eternal triangle of quality, access and cost. With conventional systems, quality often declines with an increase in access or cuts in costs. However, the appropriate use of ICT, with its potential for wider access, higher quality and lower costs, holds great promise to achieve these goals at the same time.

Education for All is the foremost priority of UNESCO, because education is both a fundamental human right and a key to sustainable development and peace within and among countries. Achieving the goals set in Dakar[3] and at the Millennium Development Summit[4] means ensuring that the digital divide does not further marginalize the poorest sectors of the population, and it entails finding creative, alternative paths to learning. It also calls for continuous reflection on ensuring that education does justice to the local context – particularly cultural, linguistic and economic needs – and the global one, in light of the reality of growing interdependence between nations.

The **third principle**, universal access to information and knowledge, especially information in the public domain, is a prerequisite for broader participation in development processes. Universal access to knowledge and information is a fundamental building block inseparable from freedom of expression. There can be no genuine knowledge societies if universal access to knowledge and information is denied. The concept of universal access is underpinned by the presence of several essential supporting components, namely: availability of com-

munication infrastructure and connectivity; available content relevant to the user; affordable services within reasonable distances; users with the necessary information literacy skills to use these services and to add value by developing, exchanging and creating new services.

As the majority of the world's population does not have access to ICT, the development of a modern ICT infrastructure should have high priority. Both commercial and not-for-profit providers should help schools, libraries, community centres, civil society organizations and government agencies to connect to the Internet, in support of universal access principles. Access to traditional media, such as radio, must also be widened as the basic building blocks of knowledge societies and their potential as relays of digital information in developing countries should be explored. Access to public domain information, also known as the "information commons" should also be encouraged. Public domain information is publicly accessible information, the use of which does not infringe any legal right, or breach any other communal right (such as indigenous rights) or any obligation of confidentiality. States should recognize and enact the right of universal online access

---

2 Article 26 of the Universal Declaration of Human Rights:

"(1) Everyone has the right to education. Education shall be free, at least in the elementary and fundamental stages. Elementary education shall be compulsory. Technical and professional education shall be made generally available and higher education shall be equally accessible to all on the basis of merit.

(2) Education shall be directed to the full development of the human personality and to the strengthening of respect for human rights and fundamental freedoms. It shall promote understanding, tolerance and friendship among all nations, racial or religious groups, and shall further the activities of the United Nations for the maintenance of peace.

(3) Parents have a prior right to choose the kind of education that shall be given to their children."

3 The World Education Forum, Dakar, Senegal, 26–28 April 2000. See <http://www.unesco.org/education/efa/ed_for_all/dakfram_eng.shtml> for more details.

4 See <http://www.un.org/millenniumgoals/> for more details.

to public and government-held records including information relevant for citizens in a modern democratic society, giving due account to confidentiality, privacy and national security concerns, as well as to intellectual property rights to the extent that they apply to the use of such information. International organizations should recognize and promulgate the right for each State to have access to essential data relating to its social or economic situation.

The **fourth principle** is cultural and linguistic diversity. In addition to art and literature, culture encompasses lifestyles, ways of living together, value systems, languages, traditions and beliefs. Cultural diversity is the common heritage of humankind and the understanding of and respect for other cultures is a prerequisite for building knowledge societies.

A central feature is the need for policies as well as actions that support plurality and diversity, so that citizens can access and create information and knowledge in their own languages and within their own cultural frameworks. The creation of environments conducive to the development of local content in digital format and the preservation of digital heritage will benefit present and future generations. Digital heritage consists of human knowledge and expression – whether cultural, educational, scientific or administrative – created on or converted to digital media. Concerted and urgent attention to this fast growing heritage is needed because of the rapid obsolescence of the hardware and software on which it is maintained. There are many constraints – economic, political, administrative, social, cultural and technical. For example, many electronic networks are currently inadequately adapted to handle the diversity of the world's languages, with only 12 languages out of the world's 6,000 or so accounting for about 90 per cent of the total web content. Two new UNESCO standard-setting

instruments, adopted in October 2003 at the last General Conference, the Recommendation on the Promotion and Use of Multilingualism and Universal Access to Cyberspace and the Charter on the Preservation of the Digital Heritage, propose strategies for addressing these challenges.

From Geneva to Tunis. The Geneva phase of the World Summit on the Information Society was a critical milestone in international co-operative efforts to promote knowledge societies and to understand their prerequisites. The Summit provided an important platform for promoting UNESCO's concept of knowledge societies. The four principles, which UNESCO took to the Summit, discussed earlier, are now reflected in the Summit Declaration and Action Plan. UNESCO is working unstintingly to maintain this momentum and to advance the WSIS process. The phase leading up to the second Summit in Tunis provides an opportunity to assess progress made since Geneva on implementation plans and actions, to explore new initiatives and solutions, and to mobilize future partners.

An Upcoming Issue: Internet Governance. An upcoming issue for UNESCO in the WSIS process is the question of Internet governance. UNESCO observes that the term "Internet governance" has not yet been clearly defined. For some, it describes the narrow issue of the management of domain names and infrastructure that are presently administered by the Internet Corporation for Assigned Names and Numbers (ICANN), a private non-profit corporation under Californian Law. The prevailing tendency in the current debate, however, is to attribute to this term a much broader meaning comprising not only technical, but also ethical, societal and legal issues. Moreover, the term "Internet governance" is misleading as it is laden with

presumptions about governing approaches which for some may imply governmental involvement.

UNESCO will continue to safeguard key values like freedom of expression, cultural diversity and openness. It will advocate that existing mechanisms such as ICANN, or any modification of these mechanisms, must reflect the following principles:

- The inherent openness of the Internet infrastructure must be preserved and should be conducive to the free flow of ideas and knowledge through word and image;
- Modifications must not result in the global Internet governance system becoming subjected to governmental control, nor should they facilitate or permit censorship;
- There must be a precise correlation between new mechanisms and the problems they seek to address;
- Technical innovation must continue to be encouraged;
- Modifications to ICANN or new mechanisms should not inhibit interoperability, cause instability, nor should they slow down the continued technical development of the Internet; and
- Any global Internet management system or mechanism must be technically competent, transparent and non-partisan.

Whichever mechanism manages the current responsibilities of ICANN, the result should be one that enables greater use of the Internet, and thereby greater participation in the modern information world, by an increasing number of citizens from diverse linguistic and cultural backgrounds.[5]

Conclusion: Constructing Knowledge Societies Together.
UNESCO is committed to fostering the creation of equitable and just societies, supporting human rights and human development in all spheres and working for achievement of the Millennium Development Goals. The necessary political, social, economic and attitudinal changes to realize these goals will not occur overnight. This will require persistent long-term actions that combine a range of multidisciplinary skills and perspectives. UNESCO has prepared a series of publications on various aspects of the WSIS[6] as well as a website[7], to inform participants of UNESCO positions and actions. UNESCO is committed to work with its partners to help implement these actions.

The challenges facing knowledge societies are those that stem from the two basic principles of UNESCO's mandate mentioned at the beginning of this article – to promote the unrestricted flow of word and image and to widen access to information. Knowledge societies should be firmly based on a commitment to human rights and freedoms, including freedom of expression. They should also help all citizens realize their cultural and linguistic rights, including the right to an education, and guarantee access to all media, traditional and new for the purposes of knowledge creation and exchange. These are long-term challenges that require analysis, investment and co-operation among States, the private sector and civil society.

---

5 For more information, see UNESCO Position Paper on Internet Governance at <http://portal.unesco.org>

6 See <http://portal.unesco.org> and type in "WSIS Document Series". Selected publications include "Cultural and Linguistic Diversity in the Information Society," "Gender Issues in the Information Society", "Social Transformation in the Information Society", *inter alia*.

7 <http://portal.unesco.org/wsis>

Steve Buckley

Whose Information Society? Communication Rights and the WSIS

Introduction. In January 2002 the United Nations General Assembly confirmed its intention to sponsor the World Summit on the Information Society (WSIS), an event to be organized in two phases – Geneva 2003 and Tunis 2005. In doing so the General Assembly stressed the urgent need to put knowledge and technology "at the service of development for all".

In the same month, a civil society coalition, the campaign on Communication Rights in the Information Society (CRIS), was launched at the second World Social Forum. The aim of the CRIS campaign was to broaden and deepen the debate on the Information Society, to promote democratization of access to communications and to strengthen commitments to communications in the service of sustainable development.

For the members of the CRIS campaign and other civil society organizations involved with the WSIS process it has been an intense period of activity which has highlighted major fault-lines in global debate on the human communications environment. During the Geneva phase, civil society actors worked closely with government delegations, lobbying on points of drafting, advising on others. Despite the holding of some key intergovernmental sessions behind closed doors, civil society participants gained a high level of insight into government positions and in some cases influenced those positions to significant effect.

The communication rights perspective is concerned with the process of human communication and with the moral and legal rights that enable us to defend our right to communicate. Of particular importance is the legally understood right to freedom of information, opinion and expression, but closely linked to communication rights are also the right to freedom of association, the right to privacy and the right to one's own culture.

But the call for "communication rights" is not a juridical quest. Rather it is a social demand for a fairer communications environment. This is a demand articulated by marginalized communities worldwide and by civil society groups concerned as much by the rise of private media concentrations and new unaccountable multinational communications gatekeepers as by the more familiar problem of authoritarian governments.

WSIS 2003 – The Geneva Phase. The idea of having a World Summit on the Information Society can be traced back to the growing economic importance of the global information and communication industries and the opening of the Internet to private commercial use accompanied by a United States vision, articulated by Al Gore, of a global "information superhighway". The European counterpoint, under the leadership of European Commissioner Martin Bangemann, spoke of the "information society" backed up by social as well as economic analysis, even including one paper with the title "People First in the Information Society".

The US and Europe built consensus in Japan at the G8 meeting in Okinawa in July 2000, which agreed the Okinawa Charter on the Global Information Society and established the G8 Digital Opportunities Task Force with the objective: "To promote international co-operation with a view to fostering policy, regulatory and network readiness; improving connectivity,

increasing access and lowering cost; building human capacity; and encouraging participation in global e-commerce networks."[1]

The Okinawa Charter was drafted at a time of economic optimism in the prospects of information technology driven economic growth. Stock markets were at the peak of the speculation fuelled dot-com boom. The Okinawa Charter and the follow-up report of the G8 Digital Opportunities Task Force strongly influenced the drafting framework for the WSIS and particularly the emphasis in the Action Plan on network infrastructure and the promotion of national "e-strategies", a term which first appears in the Charter.

At the same time, there were moves within the United Nations system to develop a strategic approach to information and communication technologies. The International Telecommunications Union (ITU) had tabled proposals as early as 1998 for a World Summit on the Information Society. In 2001 the United Nations Secretary General, at the request of Heads of State, launched the UN ICT Task Force "to lend a truly global dimension to the multitude of efforts to bridge the digital divide, foster digital opportunity and thus firmly put ICT at the service of development for all."[2]

When the UN General Assembly in January 2002 adopted a resolution endorsing a framework from the ITU for a World Summit on the Information Society (WSIS), it was in recognition of: "The urgent need to harness the potential of knowledge and technology for promoting the goals of the United Nations Millennium Declaration and to find effective and innovative ways to put this potential at the service of development for all."[3]

In contrast to the G8 position, the UN mandate was explicitly development oriented and the ITU was mandated to take the lead within a "multi-stakeholder" framework. It was agreed the Summit would take place in two phases – Geneva

in 2003 and Tunis in 2005. A WSIS Secretariat was established to support the first phase in Geneva and this included, from the start, a Civil Society Division to facilitate civil society participation.

For civil society groups such as those grouped together in the CRIS campaign, the WSIS presented a unique opportunity to engage with and raise awareness among governments and multilateral agencies and to strengthen civil society alliances and common positions. Civil society groups organized around WSIS from the earliest stage and have been vigorously present at all official preparatory meetings.

Civil society activists working in the communication environment have long recognized the social importance of access to and the effective use of communications tools. But equally there is well-founded scepticism about a narrowly drawn "Information Society" in which the key technologies are taken to mean telecommunications and the Internet.

Although much is promised by the Information Society – access to vital knowledge for health and education, better information from governments and corporations, electronic democracy, global trade and exchange, up to the minute news – many people face the danger of being left out. This danger is often called the "digital divide" by those who choose to frame the debate in terms of telecommunications and the Internet. In reality it is a broader "communications divide" characterized by the unequal access of poor people to the means of communication and to freedom of information and of expression.

In the narrow vision of the Information Society the solution to the "digital divide" is simple. It is essentially a matter

1 Okinawa Charter on the Global Information Society, Group of Eight, Okinawa, July 2000.

2 Plan of Action of the ICT Task Force, United Nations, 2001.

3 United Nations General Assembly, Resolution 56/183, 31 January 2002.

of rolling out the network infrastructure so that everyone in the world can have access to the Internet. This vision was explicit in the G8 Okinawa Charter on the Global Information Society adopted in July 2000 at the G8 Summit. It is a political-economic perspective which underpins the early WSIS texts and which in effect gives priority to building the infrastructure and the consumer base for global e-commerce over the public interest in communications for development. It does so by claiming that the former will lead to the latter without providing supporting evidence for its case.

One early draft of the WSIS Declaration described the Information Society as "a new and higher form of social organisation where highly developed ICT networks and ubiquitous access to information… improve quality of life and alleviate poverty and hunger".[4]

Others have argued compellingly that giving universal access to the Internet will cost a lot and accomplish little. Bill Gates, speaking in October 2000 at a Seattle conference on the "digital dividend", famously argued that investment in health and literacy is more important for poor people than providing access to PCs and the Internet.[5] Charles Kenny, an economist with the World Bank, has estimated that the worldwide subsidy needed for everyone living on $1 a day to get one hour of access a week might reach $75 billion – considerably more than the global total of aid flows each year.[6]

Despite such concerns, the roll-out of ICT-based products, service and applications remained a dominant perspective in the WSIS debate. This calls for market freedoms and pro-competition policies but also includes limits on freedoms and rights where this serves the interests of corporate stability and growth e.g. intellectual property, proprietary software, security, Internet governance, spectrum planning and licensing.

The CRIS campaign and other civil society participants in WSIS rejected this perspective as the basis for negotiation, arguing instead for a people-centred approach, based on human rights principles and sustainable development priorities. By the completion of the Geneva phase of the WSIS many of the concerns expressed by the CRIS campaign and other civil society groups had been adopted in the WSIS Declaration of Principles.[7] The WSIS Action Plan, however, remains largely framed in the narrow perspective.[8]

Rejection of the narrow vision of the Information Society and its assumption that ICT networks and access to information will automatically lead to the alleviation of poverty creates a serious dilemma for WSIS but one which remained unresolved at the conclusions of the Geneva Summit. If WSIS is to fulfil its mandate, it is necessary that there be sufficient analysis of the proposed actions to reasonably conclude (a) that they would indeed make a net positive contribution to the agreed development goals; and (b) that the resources deployed could not be more effectively used elsewhere.

WSIS 2005 – the Tunis Phase. The second phase of the WSIS is scheduled to end in a Summit in Tunis from 16 to 18 November 2005. There is to be a further series of preparatory meetings leading up to the Summit. The main focus of the second phase is intended to be the implementation and monitoring of the Action Plan. There are also two high level task

4 World Summit on the Information Society, Draft Declaration, Document WSIS/PCIP/DT/1(Rev.1)-E, 30 May 2003.

5 Remarks by Bill Gates, Digital Dividends Conference, Seattle, Washington 18 October 2000 <http://www.microsoft.com/billgates/speeches/2000/10-18digitaldividends.asp>

6 Charles Kenny, "Development's False Divide", *Foreign Policy*, January – February 2003 <http://www.foreignpolicy.com/issue_janfeb_2003/kenny.html>

7 World Summit on the Information Society, Declaration of Principles, 12 December 2003.

8 World Summit on the Information Society, Plan of Action, 12 December 2003.

forces under the patronage of Kofi Annan, the UN Secretary General. One of these is to deal with the contested issue of Internet governance. The other will examine the African proposals for a Digital Solidarity Fund and the wider context of financing ICTs for development.

During the Geneva phase civil society's role has been to bring critical and independent voices to the debate and, where those voices have themselves been able to find a common position through their own dialogue, to articulate that collectively to those in government. The main focus of the Geneva phase was clear – the political process leading to the intergovernmental Declaration of Principles and the Plan of Action.

In parallel, however, were a wide range of WSIS related activities and outcomes. For civil society these included meetings, conferences, announcements, partnership-based initiatives, publications and exhibitions through to counter-actions and demonstrations.

For the Tunis phase the extent and the nature of civil society engagement is likely to be significantly different. The focus of the Tunis phase is more diffuse. Governments have agreed the Tunis Summit should lead to a "political and operational statement" to reaffirm and enhance the commitments undertaken in the Geneva phase but there is unwillingness to re-open the terms of the Declaration or the Plan of Action.[9]

Having formally rejected the intergovernmental texts from the Geneva phase and with fundamental differences with governments on the framing of the Plan of Action, civil society actors who played a lead role in the Geneva phase are not in a position now to "reaffirm" the validity of governmental commitments which they never fully endorsed.

At the same time there is wide expectation that Tunis will provide a less supportive environment for civil society. Several

civil society actors have drawn attention to serious human rights violations in Tunisia and media groups have been particularly concerned with Tunisia's poor record on freedom of expression, including systematic blocking by government-owned ISPs of Internet sites critical of the Tunisian Government. Civil society participation in WSIS 2005 inevitably must also put the spotlight on Tunisia.

In addition to the drafting of a "political and operational statement" for the Tunis Summit, governments have committed to a "stocktaking" exercise, the results of which may provide a more substantive tool for measuring the effectiveness of WSIS in contributing to the development goals. The stocktaking exercise is to gather a broadly representative body of information on actions being taken by governments, private sector and civil society in furtherance of the commitments to harnessing ICTs for development.

The stocktaking explicitly requires respondents to describe the contribution that projects and actions are making to achievement of internationally agreed development goals. In this respect the results could provide a useful empirical base against which the effectiveness of WSIS commitments can be further monitored and evaluated.

Alongside the preparatory process for the Tunis Summit, two high level task forces will address the unfinished business of the Geneva phase – Internet Governance and Financing for Development. It would seem, in these fields at least, that the role and interest of civil society will continue albeit with different rules of engagement.

The establishment of the task forces by the UN Secretary General takes these fields partly outside of the WSIS process.

9 World Summit on the Information Society, Concluding statement, Hammamet, 26 June 2004.

In the case of the Financing for Development Task Force, in particular, there have already been civil society concerns expressed at the lack of transparency in the process and the absence of mechanisms for participation.

The Task Force on Internet Governance has adopted a more open and participatory methodology but there may be reluctance to open the agenda beyond a fairly narrow set of technical parameters such as the international domain name and numbering system.

Conclusions and Priorities for Civil Society. From the above it should be clear that the Tunis phase of WSIS does not have a single central focus but offers multiple points of intervention. This presents both difficulties and opportunities for civil society. In the absence of a clear external focus and goal around which to organize, civil society engagement may itself become more fragmented.

One possibility is that civil society actors who have played a lead role in the Geneva phase may simply pull back leaving new civil society actors to occupy the political space of WSIS. The resulting civil society input would probably be less critical of government and perhaps more ready to accept and work within the market-oriented paradigm.

The alternative is for civil society to "reaffirm and enhance" the civil society commitments made in the Geneva phase by building an alternative agenda to the WSIS. The best prospects for this lie with those civil society organizations and activists who have worked together in or with the campaign on Communication Rights in the Information Society.

Some principles and objectives can be drawn from the communication rights perspective and the work that has been achieved by civil society groups in the Geneva phase:

1. The market driven development of the infrastructure for access to the Internet is characterized by gross asymmetry in access to information and in information flow resulting from but also reinforcing existing social and economic inequality. In an increasingly information-based economy a more equitable access to information is essential if global social and economic inequalities are to be reduced rather than maintained or increased. This must not become a pretext for restrictions on the freedom of expression or the free flow of information but requires positive action to ensure inclusive access to communication and to defend and promote cultural diversity.
2. Universal access to communication services and networks is essential for the realization of communication rights but will not be delivered, within the foreseeable future, by providing everyone with domestic access to the Internet. Access for all to the global communications environment requires investment not only in public access centres but also in traditional communication technologies such as community radio and television. Public investment in local communications facilities is one approach. Conditionalities or levies placed upon private telecommunications providers is another. Community-based initiatives should be encouraged and supported including legal and/or regulatory reforms where there are legislative or regulatory barriers to establishment.
3. Literacy is an essential prerequisite to access and use of the Internet. Free and universal access to basic education must be ensured and supported. Media literacy and practical communications skills have become an essential component of a basic education and are necessary for the effective realization of communication rights.

4. The Internet is not intrinsically a guarantor of freedom of opinion and expression. New corporate gatekeepers have increasingly developed policies and technologies of control which go beyond the legitimate and include the arbitrary and the indiscriminate. Commercial technologies to control the Internet are also increasingly being used by governments to introduce new forms of censorship. Freedom of expression on the Internet must be protected, as elsewhere, by the rule of law rather than relying on self-regulation or codes of conduct. There must be no prior censorship, arbitrary control or unjustified constraints on the content, transmissions and dissemination of information. Pluralism of the sources of information and the media must be safeguarded and promoted including diversity in systems for information retrieval.
5. The right to privacy faces new challenges and must be protected. Every person must have the right to decide freely whether and in what manner he or she wishes to receive information or to communicate with others including the right to communicate anonymously. The collection, retention, processing, use and disclosure of personal data, no matter by whom, should remain under the control of the person concerned. Powers of the private sector and of governments to access personal data risk abuse of privacy and must be kept to a legally acceptable minimum and subject to public accountability.
6. The Internet provides enormous scope for the sharing and development of the common pool of human knowledge but this potential is increasingly held back by the reinforcement of private information property regimes in the Internet environment. There is a need for fundamental review of the international instruments governing copyright,

> patents and trademarks to incentivize development of the public domain of global knowledge, to ensure the right of access to information and the right to creative reuse and to adaptation of information, and to accelerate the social and economic benefits of freely available information including free and open source software.

The reaffirmation and enhancement of principles and priorities articulated by civil society in the Geneva phase will need a commitment to sustained partnership after the completion of the Tunis phase of the WSIS. We might call this the Communication Rights Agenda. Its focus would be on building civil society knowledge, networks and advocacy for a more people-centred communications landscape based on human rights and social justice. It may not be immediately apparent but, when we look back at the WSIS process, possibly the most significant outcome will be the extent to which the process has brought together civil society actors into the beginnings of a movement for a better communications environment that could equal the movement for a better natural environment that emerged in the closing decades of the last millennium.

Gus Hosein

Open Society and the Internet: Future Prospects and Aspirations

We once dreamed about the future. It involved a global information infrastructure that was not hampered by borders and governments. Human potential would reach beyond its prior limits as we communicated without interference in a space that was separate from flesh and steel. The Internet would set truth free, and we would follow.

And this truth and liberty are required for the maintenance of an open society. In an open society, social actors yearn for improving society, knowing that no one has perfect knowledge or control of the outcome of decisions – thus creating a space for further actors to join in and participate. It is taken for granted that actors are able to contribute, to participate, and to submit their ideas for consideration. It is far too often taken for granted that the marketplace of ideas will be filled with merchants vying for attention. It is far too often taken for granted that we have the ability to interact, to communicate, to speak freely. The Internet was supposed to be the veins through which this lifeblood could sustain an open society.

I have no intention of mocking the Free Internet image of the future. Although it is common to argue that we were ignorant when we had that dream, such hindsight is uninteresting. I am more interested in the questions of "Why did we want that dream to be true?" and "What was it that we were once seeking that we seem to be so far away from now?"

We Sought in Technology What We Were Promised. Before the popularization of the Internet, the media world was relatively stable. Film and broadcasting industries were regulated with regards to what they could show, and ratings schema applied. Print and newspaper media were regulated through liability regimes, codes of practices, and ownership regimes, amongst other forms of intervention into the marketplace of ideas. And borders were reasonable constraints on the flow of information, where books and other material could be stopped at borders in accordance with national laws.

Yet we were promised so much more, and we heard of the potential of that promise. Free speech and free expression were long heralded values, core beliefs, and rights. Freedom of speech was enshrined in constitutional documents, international charters, and sustained in jurisprudence.

The law took some time to come around, however. Consider a case in the United States, decided in the Supreme Court in 1919. The case involved five Russians in the United States who were accused of violating the Espionage Act for conspiring with the Imperial Government of Germany. The conspiracy took the form of printing, writing and distributing copies of a leaflet entitled "Revolutionists Unite for Action" and "The Hypocrisy of the United States and her Allies" that criticized the US Government's attitudes towards Soviet Russia, calling upon "workers" for solidarity and to strike, and to fight. The Court sided with the Government, contending that

> while the immediate occasion for this particular outbreak of lawlessness, on the part of the defendant alien anarchists, may have been resentment caused by our government sending troops into Russia as a strategic operation against the Germans on the eastern battle front, yet the plain purpose of their propaganda was to excite, at the supreme crisis of the war, disaffection, sedition, riots, and, as they

> hoped, revolution, in this country for the purpose of embarrassing and if possible defeating the military plans of the government in Europe.[1]

The country, after all, was at war. In a famous dissenting opinion, Supreme Court Justice, Oliver Wendell Holmes argued that the accused were not impeding the war by expressing their opinions.

> [I]t is evident from the beginning to the end that the only object of the paper is to help Russia and stop American intervention there against the popular government – not to impede the United States in the war that it was carrying on.

Controversially, he argued:

> Persecution for the expression of opinions seems to me perfectly logical. If you have no doubt of your premises or your power and want a certain result with all your heart you naturally express your wishes in law and sweep away all opposition. To allow opposition by speech seems to indicate that you think the speech impotent, as when a man says that he has squared the circle, or that you do not care whole heartedly for the result, or that you doubt either your power or your premises. But when men have realized that time has upset many fighting faiths, they may come to believe even more than they believe the very foundations of their own conduct that the ultimate good desired is better reached by free trade in ideas – that the best test of truth is the power of the thought to get itself accepted in the competition of the market, and that truth is the only ground upon which their wishes safely can be carried out.

With this statement he opened discussion on the "marketplace of ideas" and the importance of speech and contestation. Holmes's words were most surprising because he was behind two court decisions in the previous year that took harsh views of freedom of expression during war time.[2] This change of faith

reflected conversations he held with others in the meantime, and also that the war was over by the time of the decision. He concludes:

> That at any rate is the theory of our Constitution. It is an experiment, as all life is an experiment. Every year if not every day we have to wager our salvation upon some prophecy based upon imperfect knowledge. While that experiment is part of our system I think that we should be eternally vigilant against attempts to check the expression of opinions that we loathe and believe to be fraught with death, unless they so imminently threaten immediate interference with the lawful and pressing purposes of the law that an immediate check is required to save the country.[3]

In declaring this he revised his earlier opinion that falsely screaming fire in a theatre was worthy of infringing First Amendment rights to free speech, calling instead for such infringement to occur only in the case of imminent threats and immediate interference. The essence of this dissent was adopted by the Supreme Court 50 years later.

Even before that, however, the promise of speech and protecting its conditions grew greater. In a 1960 court decision in the case *Talley v. California*, the US Supreme Court upheld the right to anonymous pamphleteering. This case involved a Los Angeles city ordinance restricting the distribution of handbills. The ordinance required the naming of the person who wrote, printed, and distributed the handbill. The petitioner, Talley, was arrested and tried for violating this ordinance with handbills urging readers to boycott against certain merchants and businessmen on the grounds that they carried products of "manufacturers who will not offer equal employment opportunities

1 *ABRAMS v. US*, 250 US 616 (1919).

2 Peter Irons, *A People's History of the Supreme Court* (Penguin, 1999).

3 *ABRAMS et al. v. UNITED STATES*.

to 'Negroes, Mexicans, and Orientals'." The Supreme Court supported Talley, arguing that

> Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind. Persecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws anonymously. The obnoxious press licensing law of England, which was also enforced on the Colonies was due in part to the knowledge that exposure of the names of printers, writers and distributors would lessen the circulation of literature critical of the government. The old seditious libel cases in England show the lengths to which government had to go to find out who was responsible for books that were obnoxious to the rulers. John Lilburne was whipped, pilloried and fined for refusing to answer questions designed to get evidence to convict him or someone else for the secret distribution of books in England. Two Puritan Ministers, John Penry and John Udal, were sentenced to death on charges that they were responsible for writing, printing or publishing books. Before the Revolutionary War colonial patriots frequently had to conceal their authorship or distribution of literature that easily could have brought down on them prosecutions by English-controlled courts. (...) It is plain that anonymity has sometimes been assumed for the most constructive purposes.[4]

A similar decision emerged 35 years later that contended that there was a marketplace of ideas, as promised by Oliver Wendell Holmes in 1919. In 1995, the Supreme Court decided that anonymous pamphleteering was protected under the Constitution, in *McIntyre v. Ohio*.

> The interest in having anonymous works enter the marketplace of ideas unquestionably outweighs any public interest in requiring disclosure as a condition of entry. Accordingly, an author's decision to remain anonymous, like

> other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment.[5]

Beginning with a dissent, and then adopted into mainstream jurisprudence, free expression is considered as a key component to a functioning democracy, and something that should be upheld, promoted, and protected. This is even the case when it involves anonymous speech.

Law Unto the Internet. The printing press was heralded because it *democratized* publishing, decentralizing power to all those who owned printing presses. This was not everyone, obviously. As such, the ability of individuals to rise and speak freely was inhibited by the lack of technology available to all.

The promise of the Internet changed this. Everyone was potentially a printing press. Everyone could broadcast information, and could be the recipient of broadcasts, one-to-one, many-to-one and one-to-many forms of communications. And this was to be beyond the reach of legislatures, courts, and others who wished to impede the flow of information. And no one would know if you were a dog whilst on the Internet due to promises of privacy and anonymity. We wanted an infrastructure that could sustain our liberties, and believed that the Internet would be it.

It almost was. A most celebrated case is the fate of the Communications Decency Act, passed by the US Congress in 1996. The law required access control mechanisms on sites that made "indecent" information available to the general public, to verify the age of visitors. The constitutionality of the

4 *Talley v. California*, Supreme Court of the United States, 362 US 60, decided 7 March 1960.

5 *McIntyre v. Ohio Elections Commission*, Supreme Court of the United States, No. 93-986, decided 19 April 1995.

CDA was questioned immediately. According to David Sobel, a leading expert on the matter,

> Whether the millions of individuals visiting sites on the Internet are seeking information on teenage pregnancy, AIDS and other sexually transmitted diseases, classic works of literature or avant-garde poetry, they enjoy a Constitutional right to do so privately and anonymously. The CDA seeks to destroy that right.[6]

The US District Court injunction on the CDA used similar ideas.

> Anonymity is important to Internet users who seek to access sensitive information, such as users of the Critical Path AIDS Project's Web site, the users, particularly gay youth, of Queer Resources Directory, and users of Stop Prisoner Rape (SPR). Many members of SPR's mailing list have asked to remain anonymous due to the stigma of prisoner rape.

The Act was eventually struck down on the grounds of identity, anonymity, and free speech. According to the District Court decision, "any content-based regulation of the Internet, no matter how benign the purpose, could burn the global village to roast the pig", and this was "due to the nature of the Internet." That is,

> There is no effective way to determine the identity or the age of a user who is accessing material through e-mail, mail exploders, newsgroups or chat rooms. An e-mail address provides no authoritative information about the addressee... There is also no universal or reliable listing of e-mail addresses and corresponding names or telephone numbers, and any such listing would be or rapidly become incomplete. For these reasons, there is no reliable way in many instances for a sender to know if the e-mail recipient is an adult or a minor.[7]

At the Supreme Court, the majority concurred.

> This dynamic, multifaceted category of communication includes not only traditional print and news services, but also

> audio, video, and still images, as well as interactive, real-time dialogue. Through the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox. Through the use of Web pages, mail exploders, and newsgroups, the same individual can become a pamphleteer. As the District Court found, "the content on the Internet is as diverse as human thought."[8]

The Internet was the newest incarnation of the "press" that the Founders of the US had envisioned when they adopted the Constitution, and thus was worthy of all the protections from incursions under the First Amendment. The Supreme Court concluded:

> The Government apparently assumes that the unregulated availability of "indecent" and "patently offensive" material on the Internet is driving countless citizens away from the medium because of the risk of exposing themselves or their children to harmful material.
>
> We find this argument singularly unpersuasive. The dramatic expansion of this new marketplace of ideas contradicts the factual basis of this contention. The record demonstrates that the growth of the Internet has been and continues to be phenomenal. As a matter of constitutional tradition, in the absence of evidence to the contrary, we presume that governmental regulation of the content of speech is more likely to interfere with the free exchange of ideas than to encourage it. The interest in encouraging freedom of expression in a democratic society outweighs any theoretical but unproven benefit of censorship.

---

6 Electronic Privacy Information Center, "Internet 'Indecency' Legislation: An Unconstitutional Assault of Free Speech and Privacy Rights" (Washington DC, 1996).

7 *American Civil Liberties Union et al. v. Janet Reno* Civil Action No. 96–963, In The United States District Court for the Eastern District Of Pennsylvania.

8 *Reno v. ACLU*, 26 June 1997, 521 US 844.

The marketplace of ideas seemed secured from extraneous interference of censorship and content controls.

This all probably appears to be a bit dramatic, however. Consider the *Abrams* case: we were really talking about controversial political speech at a time of war. Certainly that deserves some constitutional scrutiny and protection. Similarly, the *Talley* case involved anonymous pamphleteering regarding racially discriminatory hiring practices at companies; and proportionately, the Supreme Court decision referred to dramatic transgressions upon expression in history as the root of oppression. But when it came to the CDA, this involved a law that merely restricted access to pornography. Why did everyone get so excited, speaking of pigs, and the marketplace of ideas, just because of mechanisms to restrict access to pornography?

My answer to that question is quite simple, and perhaps simplistic. We, and I count myself amongst those who opposed the CDA, saw this as the first step to greater controls. It is a case of the ever-articulated "slippery-slope" argument: if you begin with one form of content regulation, even with the most noble intents the rest will naturally follow. Other forms of regulation will arise either intentionally, through using the "verification" technologies to verify someone's geographic location to prevent access to non-indecent information, or less directly through the chilling of online speech for fear of surveillance or eventual censoring.

We Are Left with Strengthened Politics. Despite the "victory" in the CDA decision, the incursions upon free expression continued. Regardless of calls by experts, technologists, and lawyers that the Internet would not respond well to content regulation, content regulation followed nonetheless.

Even in the CDA decision, we were warned that the technology of the Internet could be changed. The technol-

ogy could be shaped, the structure of the market altered, to permit censorship. According to the dissenting opinion from Justice O'Connor:

> Cyberspace differs from the physical world in another basic way: Cyberspace is malleable. Thus, it is possible to construct barriers in cyberspace and use them to screen for identity, making cyberspace more like the physical world and, consequently, more amenable to zoning laws. This transformation of cyberspace is already underway. (...) Internet speakers (users who post material on the Internet) have begun to zone cyberspace itself through the use of "gateway" technology. Such technology requires Internet users to enter information about themselves – perhaps an adult identification number or a credit card number – before they can access certain areas of cyberspace much like a bouncer checks a person's driver's license before admitting him to a nightclub. Internet users who access information have not attempted to zone cyberspace itself, but have tried to limit their own power to access information in cyberspace, much as a parent controls what her children watch on television by installing a lock box. This user-based zoning is accomplished through the use of screening software (such as Cyber Patrol or SurfWatch) or browsers with screening capabilities, both of which search addresses and text for keywords that are associated with "adult" sites and, if the user wishes, blocks access to such sites.[9]

Slowly the marketplace of ideas could be chipped away at, through law, and other mechanisms.

Filtering technology emerged and is now enshrined in laws and policies in a number of countries, calling for their use at the end-user level (e.g. Australia), at service providers (e.g. US schools and libraries), and at the national level (e.g. China and Saudi Arabia). Whether through direct regulation of individuals'

9 Justice O'Connor, *Reno v. ACLU*, 521 US 844.

conduct or indirect regulation of Internet service providers, censorship is occurring. In the United Kingdom, mobile phone providers are now filtering access to pornographic content in order to prevent children from accessing these sites. An adult customer would have to contact the phone company to prove her age.[10]

There are other mechanisms, however. Notice and takedown procedures are being implemented into a number of laws in a number of countries. The United Kingdom is particularly proud of the regime for preventing access to criminally obscene material, enforced by a self-regulating Internet Watch Foundation. The IWF is now supporting other countries in copying the UK's success. But what starts with "criminally obscene" for the protection against child pornography will soon be used for other purposes. A number of countries in Continental Europe have harsh regimes to combat xenophobia by requiring the takedown of online material.

"Notice and takedown" requests are used now for the protection of "copyright". A recent study by the Dutch NGO Bits of Freedom found that, when combined with the European E-Commerce Directive that placed liability for illegal content upon website-hosting providers, the effects of copyright protection laws upon free speech are increasingly dangerous. Bits of Freedom tested ten Dutch ISPs on their practices of notice and take down by creating a number of websites quoting a text written by Multatuli, a famous author, in 1871. The text is clearly something that belongs to the public domain, and is no longer subject to copyright protection. Bits of Freedom then filed complaints to the ISPs on behalf of a fake society that was created to act as a copyright holder. Seven providers removed the text without even looking at the website, "or demonstrating any clue about copyright basics". One provider

went so far as to send all the personal details of their customer to the complainant, breaching privacy protections.[11]

Copyright laws are the creature of increased lobbying by increasingly powerful content production industries. This is a different form of politics from the politics of child protection that led to the CDA. Both political stratagems, however, rely on personal information. Simultaneously, we are seeing a return of the politics that led to the decision in Abrams, in policies and initiatives to combat terrorism. This strategy also relies on the reduction of privacy.

Politics of Surveillance-Enabled Censorship. While the CDA decision noted the challenges in requiring age verification, the minority opinion noted that technology is malleable and can be shaped to meet the concerns of those who wrote the CDA. For a reasonably-regulated Internet, all we would require is every user to disclose her name and country of residence (and even state/province), age, and then bind that information to her network information (e.g. IP address, account number at ISP).

The judges who decided that the CDA was unconstitutional argued that no such infrastructure of personal information disclosure existed at the time. The dissenting justice said that it is possible to do what the CDA envisioned. A French Court made an analogous argument in 2000 when it required Yahoo! to prevent French network users from accessing message boards where users can trade in Nazi memorabilia.

On the other hand, a US Federal court struck down a Pennsylvania law that forced Internet service providers to block access to sites thought to be distributing child pornography,

10 BBC News, "Mobile censorship" for under-18s, 19 January 2004.

11 Sjoera Nas, Bits of Freedom, *The Multatuli Project: ISP Notice & take down,* 1 October 2004.

by filtering the IP addresses.[12] Because over 80 per cent of websites on the Internet are served from IP addresses that are shared amongst sites, it was argued that the law overblocked legitimate sites. The court agreed with this contention, concluding that

> with the current state of technology, the Act cannot be implemented without excessive blocking of innocent speech in violation of the First Amendment.[13]

These three decisions all have differing conceptions of the technology. Technology can be constructed to limit access, according to the dissenters in the CDA decision and the French court, while in the Pennsylvania case the technology to limit access also limited access to protected speech, and was thus unconstitutional.

If every user was compelled to disclose this information, these regulations could work. Then if she was under 18 she could not access pornography; if she was from France, she could not access sites that trade in Nazi memorabilia. The Pennsylvania problem does not go away in her case, but if we also required that all those who speak (and set up websites) must first identify themselves, then it is likely that he would risk prosecution. It is also possible that if they both knew that this level of information was available and required in order to speak and gain access to speech, they would probably not bother in the first place. This is the way that surveillance can act as prior restraint, chilling free speech by threatening surveillance.

This is in essence what is occurring currently in the surveillance of subscriber and traffic data, but is being exhibited in two different ways on both sides of the Atlantic Ocean. In North America, under claims of copyright infringement, con-

tent-producing industry associations such as the Motion Picture Association of America (MPAA), the Recording Industry Association of America (RIAA), and the Canadian Recording Industry Association (CRIA) are approaching ISPs to demand subscriber information based on IP addresses. That is, the RIAA and the MPAA are capturing IP addresses of individual users and approaching ISPs so that they will disclose customer information, informing the RIAA and MPAA which user was using what IP address at what moment. Once legal avenues are opened to allow industry associations access to this information, these same avenues will be used by others. In so doing we will increase the use of subscriber information and other sensitive information for any number of purposes.

In Europe, the surveillance of traffic data is not yet focused on copyright infringement policies, but it soon will be, and when combined with anti-terrorism policies, it could be disastrous. Currently various governments in the European Union are establishing national policies that compel communications service providers (telephone companies [land and mobile], ISPs, etc.) to *retain* their traffic data logs. Under previous law, these service providers would have to delete this personal information once it was no longer necessary for billing or engineering purposes. Now in countries like Italy, France, and the United Kingdom, service providers will have to retain this information regarding users' e-mail, Internet and telephone habits (and locations) for periods ranging between one and five years. The UK, France, Ireland and Sweden are also pushing for this policy to be adopted at the EU, thus obliging all countries to compel all communications providers throughout

12 Tom Zeller Jr., Court Rules Against Pennsylvania Law That Curbs Child-Pornography Sites, 11 September 2004.

13 *Center for Democracy & Technology v. Pappert*, United States District Court for the Eastern District of Pennsylvania, No. 03-5051, 10 September 2004.

Europe to keep this information for a number of years, just in case one day this information is of value to law enforcement authorities.[14]

The surveillance of subscriber and traffic data is tantamount to the collection and tracking of all human conduct in the Information Society: who we speak with, who we move with, what we look for, where we receive information from, and where we send it to. As a result of these policies, European users of the Internet will have to grow accustomed to the idea that their actions will be logged for a number of years and accessible to any government that is interested, and possibly others. North American users live under the threat of their personal information being divulged to the content industry which would result in further legal proceedings. If the users are aware of these policies and mechanisms it could chill their ability to create and impart information, hampering their right to free speech. They would be less likely to consult "controversial" information for fear that it will eventually be used against them. On the other hand, if they are unaware of these policies the users will not be changing their conduct in the face of one of the largest threats to personal privacy in the modern era.

The Politics of Security-Induced Censoring. An increasingly common argument for creating structures to limit free expression is that it will aid in the war on terror. Some countries have returned to the public state of fear in which the US found itself at the time of the *Abrams* case during the First World War. Governments have called for stricter rules, greater powers, and increased funding to combat terrorism, and it was inevitable that these changes would have effects on free expression.

There are many instances of countries announcing the "takedown" of websites hosting "radical" Islamist material. In

reaction to the assassination of a Dutch film director, Belgium announced its intention to shut down certain Islamic websites and closely monitor radio programmes promoting violence.[15] A number of anti-terrorism laws introduced around the world involved curbing hate speech. In reaction to threats made on websites or the posting of messages from terrorists, websites have been removed or their contents blocked. It is likely that the website logs were also seized in this process.

One example of this is what happened to Indymedia. The Independent Media Center is an international news network of individuals, independent and alternative media activists and organizations. On 7 October 2004 its servers were seized from the London office of Rackspace, a server-hosting firm. The loss of these servers resulted in the removal of content from twenty news websites. Rackspace received a US Court order to hand over the servers in London. According to the General Secretary of the National Union of Journalists in the UK

> To take away a server is like taking away a broadcaster's transmitter. It is simply incredible that American security agents can just walk into a London office and remove equipment.[16]

The reason for the seizure remains under seal, and no US law enforcement agency has taken responsibility for the investigation into Indymedia. No UK law enforcement authorities were involved in the seizure, even though it took place in London. A public prosecutor in Italy admitted that she did request the IP logs from the server through a request to the American authorities, on grounds of combating terrorism.

14 Privacy International, *Invasive, Illusory, Illegal, and Illegitimate: Privacy International and EDRi Response to the Consultation on a Framework Decision on Data Retention*, 15 September 2004.

15 Reuters, "Mosques, Islamic school attacked in the Netherlands", *Financial Times*, 8 November 2004.

16 Indymedia UK, *Ahimsa Gone and Returned: Responses to the Seizure of Indymedia Harddrives*, 09.11.2004 19:56.

There was apparently also a request from the Swiss authorities, but this cannot be confirmed either.[17] This is the new face of censorship.

Another example of a law developed to combat terrorism that increased surveillance at ISPs is the USA PATRIOT Act, passed by the US Congress in October 2001. Under the USA PATRIOT Act, the Federal Bureau of Investigations may demand information from Internet service providers by showing a "national security letter", without any judicial oversight. ISPs are then required to comply and are gagged from disclosing their compliance. The NSLs are issued without any judicial review, or any requirement to show individualized suspicion, compelling need, and it cannot be contested.[18] The American Civil Liberties Union challenged this procedure on many grounds including that it chilled First Amendment rights. In September 2004 a US District judge agreed. Referring to *Talley v. California*, and other decisions on restraint on freedom of association,

> The Court concludes that such First Amendment rights may be infringed [...] in a given case. For example, the FBI theoretically could issue to a political campaign's computer system operator a [...] NSL compelling production of the names of all persons who have email addresses through the campaign's computer systems. The FBI theoretically could also issue an NSL [...] to discern the identity of someone whose anonymous online web log, or 'blog,' is critical of the Government. [...] These prospects only highlight the potential danger of the FBI's self-certification process and the absence of judicial oversight.[19]

The Court also argued that "transactional records" deserve privacy protection, despite existing jurisprudence on telephone traffic and bank records that leaves Internet traffic data in legal limbo:

> NSLs can potentially reveal far more than constitutionally-protected associational activity or anonymous speech. By revealing the websites on visits, the Government can learn, among many other potential examples, what books the subscriber enjoys reading or where a subscriber shops.

Without judicial review, the Court concluded, this power was unconstitutional.

Surveillance has indeed been used to limit political activity. These policies are not limited to online activity either. Surveillance has been used as a coercive measure to prevent or disable free assembly. In August 2004 the UK Appeals Courts approved of the United Kingdom Government's use of stop and search powers at protests. This involved a case where police stopped-and-searched attendees of a protest outside an arms fair in London. The police were empowered to stop and search anyone in the city of London without any precondition of reasonable grounds of suspicion. During the course of the case, it was discovered that since February 2001, this authority, granted to the Government under the Terrorism Act 2000, has been in effect on a rolling basis.[20]

Similarly, in the summer of 2004 during the American political campaign season, anti-terrorism powers were used against protestors at the presidential conventions. First the FBI would surveil activists using the Internet, and then interrogate activists before the conventions.[21] Later, at the Republican

17 Electronic Frontier Foundation, Indymedia Server Seizures <http://eff.org/Censorship/Indymedia/>

18 Anita Ramasastry, *Why the Court Was Right to Declare a USA Patriot Act Provision Dealing with National Security Letter Procedures Unconstitutional*, FindLaw Legal Commentary, 13 October 2004.

19 *John Doe, ACLU v. Ashcroft*, 04 Vic. 2614, United States District Court Southern District of New York, 28 September 2004.

20 Privacy International, *UK Appeals Court Approves Stops and Searches at Protests*, 8 August 2004.

21 ACLU, *ACLU Denounces FBI Tactics Targeting Political Protesters*, 16 August 2004.

Convention, New York police routinely fingerprinted 1,500 people arrested during the convention. This fingerprinting had the effect of delaying the release of detainees.[22]

In another American case, police installed metal detectors to scan protestors at an annual protest at the School of the Americas in Georgia. On average 15,000 people attend these yearly protests, and in the 13 years of protests, no weapons have ever been found and no protestor ever arrested for an act of violence. A week before the November 2002 protest, the City of Columbus instituted police requiring all protestors to submit to a metal detector search at a checkpoint away from the protest site. If metal was detected in the scan, the police would search through the protestor's belongings. The City claimed that the decision was due to the elevated risk of terrorist attack, prior "lawlessness", and problematic "affinity groups". The Circuit Court in this decision, known for often conservative decisions,[23] decided that the practice violated the Fourth Amendment to be free of "unreasonable search and seizures" as "there is no basis for using September 11 as an excuse for searching the protestors", and "September 11, 2001, already a day of immeasurable tragedy, cannot be the day liberty perished in this country." The Court also found that the practice violated the First Amendment by burdening free speech and association, that the checkpoints and searches were a form of prior restraint, and that the policy was content-based in that it was geared towards these protestors on this issue. Finally, the Court concluded that the search constituted "an 'unconstitutional condition;' protestors were required to surrender their Fourth Amendment rights in order to exercise their First Amendment rights."[24]

In the coming months and years more decisions will emerge from courts around the world, and they are equally

as likely to conflict with one another as they are to lead to a renewed right to free expression. Each case and every decision highlights the tightening relationship between surveillance and censorship, and the risks to privacy and free expression emerging from our responses to terrorism.

Paths to Re-invigorating the Open Society and Protecting the Marketplace. When we imagine the right to free expression, as it is enshrined in constitutional and international human rights declarations and treatises we imagine situations involving small printing presses distributing revolutionary material under an oppressive regime. Certainly the pro-Soviet Abrams and his colleagues believed that they were revolutionaries when they printed pamphlets during the First World War. Or Talley when he appealed to consumers regarding discriminatory hiring practices. Or McIntyre who insisted on publishing pamphlets despite regulations by the state of Ohio. We do not imagine people trying to download pornography, share copyrighted music illegally as champions in an oppressed world. Yet the fight for both types of people, those who are struggling against oppression and for justice, and those who wish to impart and access information are one and the same. Once we start building mechanisms to control one, the others will also be affected.

It is hard to believe, but is true nonetheless, that we need unfettered speech and privacy rights to ensure the marketplace of ideas, that will sustain the open society. Unless people can

---

22 Diane Cardwell, "City Challenged on Fingerprinting Protesters", *The New York Times*, 5 October 2005.

23 C.G. Wallace, "Screening of Protesters Unconstitutional, Court Rules", Associated Press published in *Washington Post*, 17 October 2004.

24 *Bourgeois et al. v. Peters et al.*, United States Court of Appeals for the Eleventh Circuit, No. 02-16886, 15 October 2004.

speak freely, and not be encumbered by surveillance, particularly from recent policies and practices created to combat terror, then we will not have the dream that we once had, of a place where we can all come together and communicate, separate from flesh and steel.

If we are still seeking such a world, and I think we are, then we need to fix many things. We need to understand that a zone of autonomy exists around all individuals, supported, enhanced, and protected by privacy. This will be supported through laws upholding long-respected rights to be secure from interference.

We also need to halt this alarming progression of policies and practices introduced with the intent of combating terrorism, that in the end have the effect of reducing our rights collectively. We do indeed live in perilous times, just as we did when Abrams was of issue at the end of the Great War. I acknowledge that Oliver Wendell Holmes, whom I celebrate in this paper, actually was quite unforgiving in two previous cases involving similar wartime activity, and wrote opinions condemning the accused. But I remain optimistic. Just as Holmes turned the bend and acknowledged that war does not mean the suspension of rights, and just as the US jurisprudence followed in the 1960s, and reaffirmed in the Georgia decision, rights may prevail.

If rights prevail, then the marketplace of ideas may be secured. I imagine it will be a struggle, but this is not a bad thing in itself. As Holmes noted, when speech is threatened it only reaffirms its importance. Speech is only valuable when governments try to limit it. And as he says, the "ultimate good desired is better reached by free trade in ideas." We dreamed that the Internet would sustain this marketplace, which in turn would sustain the open society. We were wrong, but our goals remain intact.

Our reasons are thus noble, as we recognize that any incursion upon free expression, even the smallest, interferes with the marketplace of ideas. This marketplace is too important to sustaining an open society to have it damaged. It offends me to see limits placed upon this marketplace, as it offends others too. And these "others" will be visionaries, coming up with legal, political, and technological innovations that may yet deliver on that dream, and bring us in from the cold.