Civil Society Background Paper

Fueling Creativity, Ensuring Consumer and Privacy Protection, Building Confidence and Benefiting from Convergence

OECD Ministerial Meeting
on the Future of the Internet Economy

Seoul, Korea, 17-18 June 2008

Hosted by 방송통신위원회
KOREA COMMUNICATIONS COMMISSION

Fueling Creativity, Ensuring Consumer and Privacy Protection, Building Confidence and Benefiting from Convergence

Recommendations and Contributions to the OECD Ministerial Meeting of 17-18 June 2008 from Civil Society Participants in the Public Voice Coalition

TABLE OF CONTENTS

1.0 Fundamental Policy Principles

1.1 Introduction

In offering these recommendations and contributions to the OECD Ministerial Meeting on the Future of the Internet Economy, civil society participants within the framework of The Public Voice Coalition reaffirm the "commitment to build a people-centered, inclusive and development-oriented Information Society, where everyone can create, access, utilize and share information and knowledge, enabling individuals, communities and peoples to achieve their full potential in promoting their sustainable development and improving their quality of life, premised on the purposes and principles of the Charter of the United Nations and respecting fully and upholding the Universal Declaration of Human Rights."[1]

Further to this, we concur with the statement of the Council of Europe submission to the Internet Governance Forum, which emphasizes the "public service value" of the Internet and links the issue of access to the Internet with the opportunity for democratic citizenship and further "that everyone should be entitled to expect the delivery of a minimum level of Internet services (for example effective and affordable access, a suitable environment for businesses to operate, etc.) irrespective of both the architecture of the World Wide Web (infrastructure, accessibility, interconnectivity) and the arrangements concerning its construction and development, with regard to the rules or principles that apply—or ought to apply—to the Internet's use (such as freedom of speech and of association, right to private life and correspondence, consumer protection, security, crime-prevention)."[2]

In the area of public infrastructure, there has been a continuing ebb and flow between those areas understood as the responsibility of public authorities, those left to the private sector, and those areas where Public-Private Partnerships (PPPs) have begun to emerge. Finding a proper balance between these approaches has been a source of continuing political debate with particular reference to transparency and accountability in the often-massive public investments required.

Of particular significance in the context of the emerging Information Society are ranges of infrastructures including technical, educational (particularly tertiary education), research, and for specific applications (in areas such as medical devices), which the public sphere finds itself for a variety of reasons increasingly constrained in its capacity to respond. However, whatever the source of the capital investment, the need for at least a degree of public financing and for overall publicly directed regulation in these investment areas is, or at least should be, unquestioned.

This is because of the responsibility of the public sphere to ensure that the objectives of social policy including equity of access and opportunity, democratic accountability and broad social inclusion are maintained. The Internet must be recognized not only as a new market

---

[1] World Summit on the Information Society. *(2003*). Document WSIS-03/GENEVA/DOC/4-E. *Proceedings from the Declaration of Principles- Building the Information Society: a global challenge in the new Millennium* [online]. *Geneva: WSIS*. Available from: http://www.itu.int/wsis/docs/geneva/official/dop.html. [Accessed 18 May 2008].

[2] Council of Europe. (2006). *Council of Europe Submission to the Internet Governance Forum held in Athens, Greece, from 30 October to 2 November 2006.* [online]. Strasbourg:Council of Europe. Available from: http://www.intgovforum.org/Substantive_1st_IGF/CoE%20submission%20to%20the%20IGF.pdf [Accessed 18 May 2008]. Please, see page 3.

infrastructure, but also as a critical social infrastructure fundamental to the realization of public responsibilities and objectives.

There remains a continuing risk of significant social and economic exclusion and discrimination resulting from a failure to recognize that publicly directed investment is necessary to support public goods in the information society (as elsewhere). Recognizing that the OECD Ministerial has the objective of stimulating a dialogue on guiding principles of the future information economy, we wish to offer the perspective that the Internet, as the paradigmatic infrastructure of the information society, must be considered as a public infrastructure and a basis for the provision of public services along with its other uses in support of, the information economy.

The Internet is the basis for a fundamental transformation in the structures and processes of modern society. It is reshaping the configuration of modern business, reconfiguring the nature of business-to-business and business-to-consumer transactions, as well as profoundly impacting the patterns of global trade and the distribution of productive enterprises. Similarly, digital processing and electronic communications have precipitated a fundamental reshaping of the structure and processes of government and the relationship between governmental institutions and citizens. Yet, just as the Internet is affecting economic and administrative life and behavior, so is it changing patterns of interpersonal connections, redistributing opportunities, and both creating new and reinforcing longstanding social and economic divisions.

Civil Society draws attention to some negative impacts of the new information economy, but also seeks to identify the opportunities which the Internet presents for overcoming inequalities, for enhancing democracy and democratic participation, for providing a means for articulating and enforcing human rights and the rule of law, and for re-balancing economic and social opportunities as between and within nations and regions.

Civil Society must work with governments, and intergovernmental agencies and private sector stakeholders in becoming the driving force within global society to ensure that those less able to realize these benefits are not left behind because of location, education, age, disability, or access to resources or infrastructure.

No initiatives concerned with the economic or business (or governmental) aspects of the Internet can take place in isolation from the social and cultural context of the Internet. Thus an active participation and contribution by Civil Society to discussions such as these within the OECD is not a favor granted to Civil Society but rather a necessary element in ensuring a worthwhile and productive outcome for all.

We recommend that all OECD member countries should support and promote:

- a policy environment in which their governments acknowledge and support in their policy, programs and regulations the necessary role that the Internet is playing as an enabler of the creation of a critical social infrastructure through which the range of services and opportunities should be made universally accessible and usable by all.

1.2 Transparency and Accountability

Transparency is a key concept linked to a modern understanding of democratic processes. Transparency implies the conduct of public affairs in an open and informative manner, so that citizens (i.e. people directly affected by the rulings) can monitor the entire process that led to the

adoption of a decision by a public authority. Transparency is an essential pre-condition to participation in the decision-making process, since meaningful involvement can only be achieved if relevant information is available and if a state of confidence is created among the participating parties. An open and bi-directional flow of information between public institutions and the wider community benefits all stakeholders, leading to more legitimate and realistic decisions and the creation of a more dynamic and active Civil Society.

Transparency of information encourages economic development by setting up the conditions for fair competition and reducing opportunities for corruption, leading to economic growth. It allows for predictability and enhanced confidence levels concerning the social environment which may, in turn, encourage future commerce and investments emerging from the trustworthiness recognized in policies and political processes.

Transparent institutions promote accountability, since responsibilities and administrative performance becomes evident in the course of monitoring these public processes, making it easier to identify flaws and to improve practices. Cooperation and involvement of all stakeholders leads to a "shared accountability" and a better and faster response to emerging issues, including natural disasters.

Ongoing dialogue and actions related to transparency and accountability are critically important at a time when public-private partnerships in the field of information and communication technology (ICT) have become an important part of the economic and political dynamic of public financing and development. Following the growth of private sector involvement in public infrastructure projects across the globe, corporate investments often become a substitute for the public funding formerly provided by inter-governmental agencies, international aid organizations, and governments. Usually considered in terms of a pooling of private and public resources, public-private partnerships aim at a cooperative provision of services and products for purposes of enhancing synergy effects. In these structures, there is a significant risk of a "democratic deficit" where the private sector involvement results in an "escape" from the accountability obligations that would apply to the public sector.

While major technology corporations are offering development support for service delivery and e-governance, they also take advantage of the newfound enthusiasm for public-private partnerships to stake out their own commercial claims and discourage alternative forms of development cooperation. Questions arise as well concerning the possible motivations of private sector "partners" in these processes as for example the gaining of inter-company competitive advantages, preferred positions in processes of standard setting (and pushing aside technological alternatives), influencing procurement strategies, and so on.

The Internet's potential for facilitating dialogue among diverse stakeholders is enabling the collaborative development of ideas regarding how to promote social and economic well-being through the development of the Internet. New tools and opportunities for effective dissemination and flows of information as well as new means for participation in debates and decision-making process has been invaluable in facilitating policy processes based in multi-stakeholder arrangements, an innovation in global policy development. In this context, the Internet Governance Forum (IGF) has emerged from the World Summit on the Information Society (WSIS) process as a promising multi-stakeholder discussion platform on public policy issues related to the development of the Internet based in principles of transparency and accountability. As stated in paragraph 48 of the Geneva Declaration of Principles:

"The Internet has evolved into a global facility available to the public and its governance should constitute a core issue of the Information Society agenda. The international management of the Internet should be multilateral, transparent and democratic, with the full involvement of governments, the private sector, civil society and international organizations. It should ensure an equitable distribution of resources, facilitate access for all and ensure a stable and secure functioning of the Internet, taking into account multilingualism".

We recommend that all OECD member countries should:

- increase the financial support to Civil Society organizations in developing countries in order to build their capacities to participate meaningfully in decision-making processes at national and international levels.
- open consultations to and increase participation of all stakeholders in all procedural stages.

We recommend that all OECD member countries should:

- adopt and implement freedom of and access to information legislation and promote an institutional culture of transparency and communication.
- open and support new communication channels, taking advantage of ICT opportunities and addressing the local social conditions and needs of users, as well as ensure equal, inclusive and effective access to these channels to all stakeholders.
- adopt adequate policies and promote partnerships to ensure the training, capacity building and necessary infrastructure for the effective use of the new communication channels by institutions, citizens and private sector.

OECD references:

- OECD. (2007). *Social and Economic Factors Shaping the Future of the Internet* [online]. Available from: http://www.oecd.org/document/4/0,3343,en_21571361_38415463_39046340_1_1_1_1,00.html [Accessed 9 May 2008].
- OECD. (2006). *Future of the Internet: Proceedings* [online]. Available from: http://www.oecd.org/dataoecd/26/36/37422724.pdf [Accessed 9 May 2008].
- OECD. (2006). Engaging Citizens in Policy-making: Information, Consultation and Public Participation. *OECD Public Management Policy Brief* [online]. Available from: http://www.oecd.org/dataoecd/24/34/2384040.pdf [Accessed 9 May 2008].

References:

- Andjelkovic, Maja (2006). Internet Governance: In the Footsteps of Global Administrative Law. (dissertation submitted, University of Kent Law School).
- Drake, William (2004). Reframing Internet Governance Discourse: Fifteen Baseline Propositions. In Don MacLean (ed). Internet Governance: A Grand Collaboration. New York: United Nations Information and Communication Technology Taskforce, 122-1613.
- OSCE. (2007). Governing the Internet: Freedom and Regulation in the OSCE Region [online]. Austria:Organization for Security and Co-operation in Europe. Available from: http://www.osce.org/item/25667.html?ch=918. [Accessed 9 May 2008].

[3] *Also available online at: www.ssrc.org/programs/itic/publications/Drake2.pdf.*

- Panos, London (2007). Panos London calls on decision-makers to commit to communication for successful development. Panos London [online]. September 2007. Available from: http://panos.org.uk/?lid=13663. [Accessed 9 May 2008].
- Salzman, James E. (2005). Decentralized Administrative Law in the Organization for Economic Cooperation and Development. Law and Contemporary Problems [online], 191-227. Available from: http://www.law.duke.edu/shell/cite.pl?68+Law+&+Contemp.+Probs.+189+(summerautumn+2005)#B1. [Accessed 9 May 2008].

1.3 Enabling ICT in Least Developed Countries

In addition to its potential for enabling individual empowerment, democractic participation and socio-economic development, the Internet offers businesses and consumers an enormously expanded marketplace, with new tools for creating, advertising, browsing, communicating, and transacting. It allows for worldwide retail commerce and instantaneous communication between buyers and sellers. It challenges geographical barriers and reduces the need for intermediaries.

Much of the attention concerning ICT use in least developed countries (LDCs)[4] has focused on the issue of "access," that is the availability of the means to physically link to the Internet or to electronically interact via the Internet through some technical facilitation of that connection. This is clearly an issue of general significance since in the absence of such a means to "connect," no other issues concerning the opportunities (or limitations) presented by Internet-enabled communications or digital processing are feasible. Specifically at the level of physical connection the issues of the availability (and usability) of such access through facilities that are geographically convenient and within the financial means of even the poorest present overwhelming arguments for publicly initiated and supported "access facilities."

At the larger system level, the linkage of local service provision to the global telecommunications network remains a cause for concern by many countries, particularly in sub-Saharan Africa. These issues are being continuously redefined as the capacity of the global network responds to the ever-escalating requirement for additional capacity (bandwidth) driven both by increased numbers of users and by increasingly bandwidth-intensive applications and content.

Additionally, those involved in development increasingly have come to the realization that the Digital Divide is often but a symptom of other "divides" limiting accessibility to Internet-based services. These divides reflect disparities in literacy and numeracy, location and geography (with rural and remote areas being particularly ill-served), education and skill levels, gender, and physical ability.

Industrialized Countries are using skilled or (in some cases privileged) access to knowledge, capital, and an existing advanced technology infrastructure to realize enormous benefits for themselves and their organizations through the use of the Internet and related technologies. As well, these technologies are providing enormous benefits to consumers and to the range of users. The challenge in LDCs is to extend to the widest possible range of users the opportunities presented by ICT.

[4] Members of Civil Society associated with this report use the "least developed countries" (LDCs) terminology for convenience and readability purposes only, in reference to its use in the context of the OECD and the UN. We understand this expression to refer to least economically developed countries (LEDCs) and do not accept that economic development determines the quality of social and cultural development within a country or region.

There is an urgent need for citizens around the world to have ready and equitable access to the Internet and the means to use the Internet in productive and meaningful ways.

Civil Society also recognizes the exceptional difficulties (and opportunities), which characterize Indigenous Peoples' experiences with ICT development. In many cases Indigenous Peoples suffer a cascade of difficulties in relation to their participation as equal partners in the Information Society and knowledge economies. Indigenous Peoples are disproportionately found in rural and remote areas. Their traditional groupings often straddle national boundaries, and their traditional geographic locales are often in areas of particular environmental or economic vulnerability. As well, their traditional languages and cultures distinguish them from others in their societies. In these contexts, access to ICT and the Internet often present there are significant barriers to ICT and the Internet access. Yet, it is precisely through the use of ICT that impoverished economic and social conditions can most effectively be alleviated. ICT provide a potential means through which Indigenous Peoples may participate as equal members in the larger society and realize their aspirations for self-management and self-determination. Civil Society supports the provision of exceptional support for Indigenous Persons to realize the opportunity for access and effective use of ICT in support of their objectives.

The Internet also allows for the distribution of intelligence and empowerment to the edges of the network. Thus, there is a natural correspondence between ICT and local self-management and empowerment and it provides the means for effective participation by grassroots and other communities in broader economic, social and political processes. Civil Society believes that these potentialities should be recognized and supported in the design and deployment of technical and related organizational and governance systems.

There has been a decline in the cost of computing hardware in LDCs as elsewhere[5]. While this development brings access to personal computing into the income range of a larger number of persons in the developing world, it also serves to highlight the excessive cost of Internet access in many of these same countries, resulting from, for example, managed pricing or lack of competition.

Many of the services which have been computer-based in Industrialized Countries are cellular telephone-based in LDCs. Electronic funds transfer, electronic purchasing, rapid information transfer concerning local markets and so on have now, through popular use (and popular innovation) become cellular services.

Also, while not generally understood under the rubric of ICT, Community Radio is nevertheless one of the most effective tools available for information dissemination and community involvement. Notably new organizational and technology developments (including linkages with the Internet) have extended the capability of Community Radio.

As noted elsewhere, ICT have the potential to be transformative in a number of ways including through providing enabling mechanisms for emerging beneficial processes and for linking new

[5] For example, the One Laptop per Child personal computer among other devices.

technologies with the range of activities supported through Development Assistance programs which too often are reflective of stale and long outdated organizational divisions.[6]

We recommend that all OECD member countries should support and promote:

- enhanced access to new technologies by LDCs through development assistance programs, the development of the regulatory and policy processes in LDCs, and a commiment in this direction comparable to the Overseas Direct Investment.
- widespread access to the Internet through publicly supported public and community Internet Access points where appropriate.
- lower costs of interconnection for LDCs.
- equitable access to the benefits and services of the Information Economy and Society through the amelioration of the variety of social divides including the "digital divide" but also differential Internet access resulting from differences in levels of literacy and numeracy, location and geography (with rural and remote areas being particularly ill-served), education and skill levels, gender and physical ability.
- opportunities for the effective use of ICT to support the range of community and individual activities, services, opportunities for innovation and creative production among others.
- the provision of exceptional support for Indigenous Persons to realize the opportunity for access and effective use of ICT in support of their objectives.
- implementation of nationally appropriate means for reducing Internet access costs and increasing Internet capacity in LDCs (as elsewhere).
- empowerment at the edges of the network through the deployment of appropriately designed technical and related organizational and governance systems.
- the delivery of the range of services in support of the Information Economy and Society through cellular telephones in LDCs.
- the development and licensing of Community Radio initiatives as required, by lobbying for changes in legislation and regulation at the national level in LDCs to enable the development of local and community radio stations.

1.4 Equitable Participation and Non-discrimination

As already noted, the Internet Economy is transforming many of the structures, systems and services of contemporary commerce and governance. It is providing unprecedented opportunities for the development of new types of services and for very significant wealth creation. However, at the same time, traditional commercial service delivery and supply channels are disrupted and there are significant ongoing redistributions in opportunities for employment.

Overall, and in most spheres of life in Industrialized Countries, the Internet and digital processing are providing the underlying infrastructure through which work is undertaken. What this means is that access to and the means for participation in economic (among other aspects of) life may be directly dependent on equitable access to the opportunity to utilize this infrastructure as a source of employment, as a means for the conduct of information and commercial transactions, and as

[6] Portions of the text regarding LDCs have been drawn from Gurstein, Michael. 2007. "Editorial: Some Thoughts on ICT in a Developing World Context," Journal of Community Informatics, vol. 3, no. 4. http://cijournal.net/index.php/ciej/article/view/484/384

the conduit through which productive activity and participation in the Internet economy may take place.

The absence of equitable means for such participation; or the existence of formal, informal or even invisible barriers to such participation, may be highly damaging to the opportunities and prospects for individuals to carry on their lives in ways similar to their neighbors who do not suffer such discrimination or face such barriers.

As noted, the matter of discrimination with respect to "access" and thus the "Digital Divide" can be re-interpreted as including elements of inequitable access as a consequence of gender, location, or disability, among others. Such barriers or forms of discrimination may occur and be equally damaging if they interfere with individual (or collective) opportunities for the use of the Internet both for purposes of "consumption" (of information, entertainment, knowledge, communication); production (of information, services, creative artifacts); or for transactions (financial, commercial, interpersonal).

As a platform which is fundamental to the organization of the basic structures of modern society and contemporary economies the matter of equitable and non-discriminatory access is an essential component to be included in an e-economy or e-government policy framework.

Barriers to equitable participation include the following:

Differential access to the use of the Internet may be a result of the cost of access (Internet access costs or costs of the input/output devices themselves—personal computers for example). Many of those currently not using the Internet are not doing so because of the cost of this service. While low or minimal cost home computer and Internet access is becoming increasingly feasible with the ready availability of very low cost computers. ensuring the widespread availability of publicly accessible Internet services at no or nominal cost (through community access points or telecentres) remains a minimum basis for ensuring equitable participation in the Information Society.

In many circumstances, there are additional difficulties (and costs) in obtaining access to the means for participation in the digital economy by those living in remote, rural, or low-income areas and particularly for Indigenous Peoples. The exceptional cost of the provision of enhanced (broadband for example) infrastructures in such areas may lead to gaps in access in these areas if the service provision is left solely to market considerations. In order to ensure that there is no discrimination or additional barriers to participation by residents of rural and remote regions it may be necessary for public authorities to intervene to find means to balance costs as between locales.

Disability interferes with the opportunity to make use of the input/output devices through which the digital platform is accessed. Such disabilities might include visual disabilities (the inability to read or interpret messages on a screen), colour blindness or other forms of visual impairment; hearing impairment (the inability to identify sound cues for certain types of actions); or palsy (which would limit the use of normal input/output devices) and so on. There are a variety of well recognized standards for the design of web interfaces which enable utilization by those with visual and other disabilities but these standards are for the most part voluntary and frequently are ignored or overlooked. The enforcement of these standards, particularly in government sites or sites which are supportive of public participation, provide public services, or are overall in the

realm of "public activities," should become mandatory and means for their enforcement should be developed. Barriers of disability may also occur where public Internet access points are inaccessible because of physical barriers (as for example not being wheel chair accessible), then the opportunity to participate is doubly restricted.

Elevated levels of literacy may be implicitly required by certain digitally enabled activities. This may discriminate against those with lower levels of education, cognitive abilities or limited facility with the language being used for the service. Similarly as with visual disabilities standards exist for determining the level of literacy required for utilization of specific sites and these should be formally adopted and means developed for their enforcement particularly in those sites necessary for social, political and economic functioning in the Information Society.

Further, many of those who do not make use of the Internet may be suffering from a lack of knowledge or personal confidence with respect to Internet or ICT use. This would be particularly the case for the elderly and those with lower levels of education. The barrier of lack of confidence or skill with respect to Internet use may be overcome through the availability of training or support services in the context of the PIAPs.

Equitable gender access to ICT has been linked to an increase in overall social equality for women; however, within numerous global contexts—including those of Industrialized Countries—gender disparities in access to ICT persist, and women predominate in the lower-wage sectors of the information economy. Women also are under-represented in ICT decision-making capacities. Gender is one of many factors that determine the impact of ICT on women's lives. Ethnicity, religion, age, physical ability, and socio-economic status also figure into the degrees of inclusion and exclusion that differentiate regions and communities. Key to overcoming the barriers, shortcomings and misconceptions that exacerbate gender inequalities in ICT are the comprehensive education of all persons regardless of gender, the promotion of equal access for women to scientific and technological arenas, the provision of opportunities for lifelong learning in ICT, and the augmentation of women's roles in ICT decision-making.

We recommend that all OECD countries should support and promote:

- Enforceable standards for the design of web interfaces which enable utilization of these sites by those with visual and other disabilities and the implementation of the means for enforcement of these.
- Standards for the level of literacy required for utilization of specific sites and particularly public service sites and the implementation of the means for enforcement of these standards.
- The widespread availability of publicly accessible Internet services through the availability of low cost Internet access and through community access points or telecentres at no or nominal cost.
- Training or support services in the context of the Public Internet Access sites to assist those who lack confidence or skill with respect to Internet use.
- Policies and programs for comprehensive education for all persons regardless of gender; the promotion of equal access for women to scientific and technological arenas; the provision of opportunities for lifelong learning in ICT; and the augmentation of women's roles in ICT decision-making.

- Policies and programs to ensure that there is no discrimination or additional barriers to participation by residents of rural and remote regions and where necessary intervention to balance costs as between locales and regions.

OECD references

- Organization for Economic Cooperation and Development. 2001. Understanding the Digital Divide. Paris: OECD Publications. Available from: http://www.oecd.org/dataoecd/38/57/1888451.pdf [Accessed May 19, 2008]

References

- Abdul Rahim, R. et al. (2005). Access, Empowerment & Governance: Creating a World of Equal Opportunities with ICT. Kuala Lumpur: Global Knowledge Partnership.
- Association for Progressive Communication (APC) and Instituto del Tercer Mundo (ITeM). (2007). Global Information Society Watch [online]. Available from: http://www.globaliswatch.org/download [Accessed May 19 2008].
- Association for Progressive Communication. (2006). Internet Rights Charter: Internet for Social Justice and Sustainable Development [online]. United States: Association for Progressive Communication. Available from: http://rights.apc.org/charter.shtml. [Accessed May 19 2008].
- Gurumurthy, Anita and Singh, Parminder Jeet (2005). Political Economy of the Information Society: A Southern View [online]. Montevideo, Uruguay: Instituto del Tercer Mundo. Available from: http://wsispapers.choike.org/papers/eng/itfc_political_economy_is.pdf. [Accessed May 19 2008].
- Hafkin, Nancy. (2004). Paper Presentation: Gender Responsive Information Society. Proceedings of the United Nations ESCAP High Level Intergovernmental Meeting to Review the Implementation of the Beijing Platform for Action and its Regional and Global Outcomes in Bangkok. Thailand: United Nations ESCAP.
- Huyer, S. and Sikoska, T. (2003). Overcoming the Gender Digital Divide: Understanding ICT and Their Potential for the Empowerment of Women. INSTRAW Research Paper Series, No. 1. Dominican Republic: United Nations-INSTRAW.

2.0 Fueling Creativity

2.1 Access to Knowledge and Public Domain

The Internet is global; it has penetrated the farthest reaches of our world and has done so quickly. Our digitally networked environment promises to affect even more aspects of our daily lives in the future and in every part of the world. In this context, the Internet allows for much greater A2K (Access to Knowledge) through new wealth generated in the transition to a global knowledge economy and the democratizing freedom enabled by the information society. A2K is a critical component of information policy, rooted in human development and human rights and also in the demands of social justice, distributive equality, and identity politics. Access to knowledge is the normative foundation of an information age conscious of the social responsibility embedded in our technological infrastructures.

Legal restrictions on information flow and knowledge sharing shape how markets work in today's globalized world. IP (Intellectual Property) laws have been the center of attention in the knowledge economy because it is the legal regime most readily available to extract revenue from the knowledge and information components of technology. The objective of IP law is to balance the need to provide incentives to creators and owners and the benefits derived from allowing the general public to access and use those works. This balance is especially crucial for the collaborative processes of the participative web. A2K and the various public interests, of which it is composed, are seriously hindered by the expansion of the exclusive rights of IP at the expense of public access. This tension between the public and private interest in knowledge production becomes more urgent when IP protection frustrates access to public goods such as science, education, and culture.

We recommend that all OECD member countries should:

Science

- enact legislation excluding facts and data from proprietary ownership.
- ensure that publicly-funded research be made accessible to the public.
- invest in distributed network infrastructures for public research institutions.

Education

- adopt meaningful exceptions to and limitations on copyright for educational and library uses and for the benefit of people with disabilities.
- promote the procurement of open educational resources in public schools.
- build infrastructure and capacity for Internet access in poor and rural areas.

Libraries

- create robust exemptions for the circumvention of DRM (Digital Rights Management) for libraries and research.
- engage public-private partnerships to enable affordable access to information.
- support the digitized preservation of historical and cultural materials.

Culture

- regulate the concentration of media ownership to protect the public sphere.
- make government-funded media and arts available for free online.
- safeguard innovative peer distribution and production technologies.

2.2 Innovation and Copyright

The Internet has made available new opportunities for creativity, community, and access to government. Video hosting platforms like YouTube have democratized the creation and distribution of film. YouTube now hosts over 6.1 million videos and over 100 million videos are being viewed each day - making a total of over 3.65 billion views per year. By comparison, the U.S. film industry released 607 movies and sold a record of 1.45 billion cinema tickets in 2006[7]. The Internet has also transformed our notions of culture and civic discourse and has empowered

[7] Motion Picture Association of America. (2005*). Research & Statistics – Frequently Requested Statistics* [online]. Available from: http://www.mpaa.org/researchStatistics.asp. [Accessed 29 February 2008].

ordinary citizens to be heard alongside well-funded lobbyists. U.S. Presidential candidates have used YouTube videos to distribute their policy statements and to woo voters. Citizens have created and uploaded their own videos explaining why they support particular candidates and policies. In Canada, and elsewhere, concerned citizens have uploaded self-made videos petitioning government representatives on such topics as the need for balanced copyright law reform.

Because it is global in reach, the Internet also has the potential to be a powerful tool for distance education across national borders, for network and capacity building, for cultural exchange, and facilitating economic and social development. But while the Internet is global in scope, it is also currently rooted in a physical infrastructure that makes it extremely sensitive to national legal regimes and regulatory practices. The future growth of the Internet and its ability to reach its full potential value in the economic, cultural and social spheres depends on OECD countries adopting legal regimes and regulatory frameworks that provide appropriate incentives for investment in the development of Internet technologies and the widespread deployment of broadband infrastructure while safeguarding the rights of consumers and citizens.

In particular, it is essential that national and international copyright laws provide an environment that is conducive to innovation. This is crucial for information users and suppliers, such as students, educators, universities and libraries, which must rely on specific exceptions and limitations in national copyright law to make effective use of the Internet and ICT. It is also important for broadband uptake at the infrastructure level. Internet service providers need a predictable legal environment to manage risk and attract investment. It is necessary for the development of new Internet technologies, such as search engines and content hosting platforms, which offer these new possibilities for fueling creativity, community building and civic participation.

The current global legal environment poses a number of policy challenges both for Internet intermediaries and those seeking to use technology in order to foster economic and social development. First, copyright law regimes across different countries contain varying exceptions and limitations. Second, there is little agreement and divergent case law about the application of private international law and conflict rules in the Internet. This makes it difficult to assess the potential legal liability Internet intermediaries may face in offering innovative cross-border services and reducing the availability of technologies in countries that could use it most optimally.

Many OECD countries have adopted special legal regimes for Internet service providers and other Internet intermediaries, limiting their potential legal liability for copyright infringement and defamation. These rules were adopted in recognition of the social importance of fostering Internet connectivity and networked communications. Now, as more and more of our cultural and civic life is lived online in discussion forums, wikis and social networking communities, these rules have come to have even greater significance.

The U.S. Copyright Act contains four "safe harbors" for Internet intermediaries' routine activities: acting as a conduit of Internet communications, caching of browseable material, hosting of user created content and provision of information location tools and search engines (17 U.S.C. §512). European Community law contains a similar set of limitation of liability provisions for information society services and providers which provide connectivity, cache content, and host user-created content (EU eCommerce Directive, 2000/31/EC, Articles 12-15). These regimes

created a relatively stable environment for innovation. That, in turn, facilitated the development of robust hosting platforms (such as YouTube, and Wikipedia), as well as a rich world of user created content, global economic enterprises (eBay) and powerful search tools (Google, Yahoo!).

However, that environment is now under threat from various sources. First there has been a noticeable movement towards characterizing temporary and transient reproductions of digital copyrighted material, such as that in computer memory, as copyright infringement. This view was adopted, somewhat controversially, in the U.S. National Information Infrastructure Taskforce's landmark 1995 White Paper, which recommended that Internet Service Providers be held directly liable for copyright infringement for their role in passing communications across their networks. Since communications on the Internet involve serial reproduction and distribution of digital material, this would have translated into potentially unmanageable liability for Internet Service Providers and Internet intermediaries. Although it is clear that there is no international consensus on this point, recent bilateral trade agreements have required U.S. trading partners to adopt the U.S. position. This has increased the potential scope of direct copyright liability for Internet intermediaries across the globe and stifled technological development and investment in countries where there are no countervailing limitation principles (such as the U.S. fair use doctrine) or exceptions for intermediaries.

Second, copyright owner industry groups have attempted to overturn the balance struck in the existing copyright safe harbor and limitation of liability regimes, in efforts to clamp down on perceived widespread online copyright infringement. These efforts endanger fundamental privacy rights of Internet users and threaten the end-to-end principle that is central to the Internet's open architecture. Reflecting a seminal case in the early days of the Internet, the U.S. safe harbor regime specifically states that ISPs and Online Service Providers (OSPs) are not required to monitor nor affirmatively search for evidence of potential infringement on their networks (17 USC §512(m)). Similarly, Article 15 of the EU eCommerce Directive states that information society service providers have no general obligation to monitor communications on their network.

Despite this, major film and music copyright industry groups in Europe have recently advocated for a suite of proposals that seem to jeopardize the spirit of that framework principle.

A lobbyist memorandum produced by the International Federation of Phonographic Industries and circulated to European Parliament staffers in November 2007 calls on the European Parliament to mandate that ISPs block communications using particular Internet protocols, install network-level filtering and block access to websites that facilitate copyright infringement[8].

In December 2007, a proposed amendment to a European Parliamentary committee report required ISPs to filter their networks and customer communications in order to find evidence of potential infringement. If adopted, these proposals are likely to radically alter the current nature of the Internet. ISPs and Internet intermediaries will be obliged to monitor their networks in an unprecedented manner. This makes it more likely that ISPs will be deemed to have constructive knowledge of online copyright infringement taking place on their networks, thus, disqualifying them from the safe harbors that have previously safeguarded their businesses. At the same time, adopting such filtering measures is not likely to be technologically effective because encrypting communications can defeat them. Thus, mandatory network filtering is not likely to reduce online

[8] IFPI. (2006). *ISPs – Technical Options for Addressing Online Copyright Infringement* [online]. Available from: http://www.eff.org/files/filenode/effeurope/ifpi_filtering_memo.pdf. [Accessed 9 May 2008].

copyright infringement, but is likely to result in invasion of all Internet users' privacy, particularly if it requires deep packet inspection.

France has proposed draft legislation for a "graduated response" requiring ISPs to terminate the Internet access of customers on the basis of a rightsholder allegation of repeat copyright infringement and to exchange lists of "blacklisted" Internet users to whom Internet service cannot be provided. Similar proposals have been adopted in Japan, and are being discussed in the U.K., Canada and Australia, and have been rejected in Sweden. In the digital age, excluding citizens from the ability to connect to and communicate on the Internet, amounts to cutting off individuals from civic and cultural life. This is a disproportionate response to the harm involved. The penalty imposed is far more severe than traditional copyright monetary sanctions, both for the individual involved, and also for society at large. Adopting such a response to meet the needs of one group of rightsholders is likely to create social division and to detrimentally impact the development of the Internet's global infrastructure for all humankind.

In the United States, well-established principles of copyright law that balanced the needs of new innovators with those of rights holders are under challenge. In a series of cases against developers of peer-to-peer software, rights holders have asked courts for orders requiring the redesign of multiple purpose technologies and a veto power over particular features. U.S. courts have made it clear that the burden of copyright enforcement falls on rights holders and not the providers of new ICTs. As the Ninth Circuit Court of Appeals recently stated: "The DMCA notification procedures place the burden of policing copyright infringement—identifying the potentially infringing material and adequately documenting infringement—squarely on the owners of the copyright.[9]" Despite that, major copyright owner industry groups have begun litigation against Internet search engines and user-created content hosting platforms, such as Google's YouTube, Veoh, MyMP3Tunes.com, and iMeem, thus challenging the validity of the safe harbor regime.

These copyright-driven initiatives are already impeding investment in ICT research and development, and reshaping the technology innovation environment in OECD countries. In the longer term, they are likely to stifle Internet innovation and to reduce the availability of ICT that may fuel creativity, build communities, empower civil engagement, facilitate distance education, and foster economic and social development across the world.

We recommend that the OECD should:

- undertake research to identify which national legal regimes treat temporary and transient reproductions of copyrighted works as copyright infringement, for which Internet intermediaries may be held directly liable, and whether those countries' legal regimes also provide for safe harbor regimes or limitations on liability for Internet intermediaries.
- undertake research to determine the economic value attributable to the existence of safe harbor regimes in those OECD countries that treat temporary and transient reproductions of copyrighted works as copyright infringement, and have such safe harbor regimes.
- undertake comparative analysis of the different ISP safe harbor and limitation of liability regimes in use in OECD countries, and produce best practice recommendations on legal norms and policy practices for countries considering implementation of legislative

[9] Cited in EFF Internet Law Treatise. (2007). Perfect10 v. CCBill, Case Nos. 04-57143, 04-57207 (9th Cir. March 29, 2007) [online]. Available from: http://ilt.eff.org/index.php/Perfect_10,_Inc._v._CCBill_LLC. [Accessed 29 February 2008].

limitation of liability regimes, and entities within OECD countries that are developing policies and practices to implement such legal regimes.

We recommend that all OECD members countries should be:

- encouraged to implement robust safe harbor regimes for Internet intermediaries, and to introduce reduced penalties for Internet intermediaries that act in good faith and without knowledge of specific copyright infringement, in order to foster technological innovation and investment in ICT infrastructure that will benefit all humankind.
- protect their citizens' privacy rights by upholding the foundational principle that ISPs and Internet intermediaries are not required to monitor communications on their networks in any circumstances.

References

- Electronic Frontier Foundation (2008). *Fair Use Principles for User Generated Video Content* [online]. Available from: http://www.eff.org/issues/ip-and-free-speech/fair-use-principles-usergen [Accessed 18 May 2008].
- Jonathan Band and Jenny Marcinko. (2005). *A New Perspective on Temporary Copies: The Fourth Circuit's Opinion in Costar v. Loopnet 2005 STAN. TECH. L. REV.P1* [online]. United States: Stanford Technology Law Review. Available from: http://stlr.stanford.edu/pdf/Band-Costar.pdf. [Accessed 22 May 2008].
- Edwards, L. and Waelde, Charlotte, Ph.D. (2005). Online Intermediaries and Liability for Copyright Infringement, Report Prepared for World Intellectual Property Organization Seminar on Copyright and Internet Intermediaries. Geneva: WIPO.

OECD Resources

- OECD Directorate for Science, Technology and Industry, Committee for Information, Computer and Communications Policy. (2005). *Working Party on the Information Economy, Digital Broadband Content: Music Report DSTI/ICCP/IE(2004)12/FINAL* [online]. Available from: http://www.oecd.org/dataoecd/13/2/34995041.pdf. [Accessed 9 May 2008].

2.3 Freedom of Speech and Information

Article 19 of the Universal Declaration of Human Rights states:

"Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers[10]."

The growth of the Internet and Information and Communications Technologies enables those freedoms to escalate at an even greater extent. Individuals are now able to easily speak to the general public outside of their immediate geographic location. The Internet not only facilitates the

[10] United Nations. (1948). *Universal Declaration of Human Rights -Adopted and proclaimed by General Assembly resolution 217 A (III) of 10 December 1948* [online]. Available from: http://www.un.org/Overview/rights.html. [Accessed 9 May 2008].

expression of thought and opinion; it also enhances the ability for individuals to find and to receive valuable information and opinions to further knowledge, culture, discussion, and debate.

However, as much as new technologies can enable further expression and transfer of creativity and information, they can just as easily restrict it. Since users of the Internet must rely upon infrastructure to communicate online, those who control access to the Internet can also exercise technical control over what content appears online, and who may send or receive it. Because of the global forum that online discourse can give to individuals, it is vitally important that the freedom of opinion and expression be preserved online.

Barriers to online freedom of expression can take any number of forms, and can be erected at a number of points in the chain of communication.

Disfavored content might be censored by governments, enjoined by private parties through litigation, or removed by network providers or hosting services. This disfavored content might include criticism, unpopular views, or traffic or services that may compete with the censoring entity. Other restrictions on speech include mandatory identification requirements that prevent anonymous speech or subject speakers to greater monitoring and surveillance. There is a history both of technical restrictions on disfavored content[11] and through frivolous defamation or intellectual property litigation[12].

We recommend that all OECD member countries should:

- ensure that the freedom of speech is not unduly constrained, whether by technical means, or the abuse of legal process.
- Ensure a regulatory framework that respects and supports freedom of expression, both in conveying and receiving creative content and information. This is of paramount importance in any policy-making that touches on individuals' ability to communicate and create online.

References:

- Ronald Deibert, John Palfrey, Rafal Rohozinski and Jonathan Zittrain (eds). (2008). *Access Denied: The Practice and Policy of Global Internet Filtering*. Cambridge: MIT Press[13].

3.0 Ensuring Consumer and Privacy Protection and Building Confidence

In addition to its potential for individual empowerment, democracy, and socio-economic development, the Internet offers businesses and consumers an enormously expanded marketplace, with new tools for creating, advertising, browsing, communicating, and transacting. It removes

[11] See section 4.2 on net neutrality.

[12] See sample cyberSLAPP.org. *Don't chill online freedom of expression*. [online]. Available from: http://www.cyberslapp.org/about/page.cfm?PageID=7. [Accessed 9 May 2008].

[13] *Also available online at http://opennet.net/accessdenied.*

geographical barriers, reduces the need for intermediaries and allows for instantaneous communication between buyers and sellers.

However, the promise of electronic commerce recognized by OECD countries in 1998 has not been fully realized. Despite the fact that current technologies and communication networks give unique possibilities to achieve a truly global market, cyberspace continues to be largely carved along national and geographical lines as businesses continue to segment markets and search engines drive consumer choice towards a home and language bias.[14]

Electronic commerce has also brought a host of new challenges that undermine consumer confidence, including online fraud, lack of data protection, unwanted and intrusive marketing techniques, unfair contracting methods and terms, and ineffective cross-border dispute resolution. As these practices continue to plague the electronic marketplace, there is a risk that initial consumer confidence in the medium will be seriously damaged. Indeed, there is evidence that consumers are not engaging in e-commerce for these reasons.[15]

OECD countries have made significant progress over the past decade in addressing obstacles to consumer confidence online, in particular by enacting consumer protection laws related to electronic commerce, data protection and spam. However in many countries lack of government resources, infrastructure and staff training result in poor compliance and enforcement.

There remains much to be done if consumer confidence is to be maintained, let alone increased. Therefore we ask the OECD and its member governments to be more active in enforcing existing laws and regulations that protect the rights of consumers. And we urge OECD governments to commit to defend essential Consumer Rights in the Digital Environment at the Future of the Internet Ministerial.

3.1 Consumer Rights in the Digital Environment

In the digital world consumer protection laws (and related regulations) are no longer adequate to protect consumers in their everyday dealings with business. While business models are changing to take advantage of technical developments, consumer policy has not kept pace. Work is needed to define consumer rights, especially in the context of digital products, which are not included within the scope of consumer protection law in many OECD countries.

---

[14] See Fielder, A. (2007). Making the European internal market work for consumers in National Consumer Council. *National Consumer Council* [online]. Available from: http://www.ncc.org.uk/nccpdf/poldocs/NCC158ft_european_internal_market.pdf . [Accessed 9 May 2008] or see Eurobarometer (2006). Internal Market, Opinions and experiences of Citizens in EU-25 [online]. Available from: http://ec.europa.eu/public_opinion/archives/ebs/ebs_254_en.pdf. [Accessed 9 May 2008]. See also European Parliament (2006). Refusal to Serve Consumers because of their Nationality or Residence – Distortions in the Internal Market for E-commerce Transactions*? DG Internal Policies of the Union, Policy Department Economic and Scientific Policy* [online]. Available from: http://www.ivir.nl/publications/helberger/ecommerce_en.pdf. [Accessed 9 May 2008].

[15] See Smith, A.(2004). Cybercriminal Impacts on Online Business and Consumer Confidence. Information Review 23.3 [online]. Available from: http://www.emeraldinsight.com/Insight/ViewContentServletFilename/Published/EmeraldFullTextArticle/Pdf/2640280306.pdf. [Accessed 9 May 2008]. Also Trans Atlantic Consumer Dialogue (2007). Consumer survey, Resolution on Internet Security and TACD Resolution on Identity Theft, Phishing and Consumer Confidence. Available from: http://www.tacd.org. [Accessed 9 May 2008].

For instance, it is in the public and consumer interest to ensure a fair return for creative endeavor in the digital environment. The key word, however, is "fair". Digital Rights Management Systems (DRMs) should expect public support only to the extent that DRMs respect the wider interests of public access, consumer rights, privacy safeguards, and the promotion of competition and technological development. In particular, the potential anticompetitive effects of DRMs should be reviewed.

We recommend that all OECD member countries should:

- Ensure that consumer protection laws are properly enforced and cover digital products to the same extent that other consumer goods and services are covered. The following consumer rights should be defined in OECD agreements and guidelines:

    - Right to the principle of "technical neutrality"
    - Right to benefit from technological innovations without abusive restrictions
    - Right to interoperability of content and devices
    - Right to the protection of privacy
    - Right not to be criminalize
    - Right to choice, knowledge and cultural diversity
    - Right to defend and maintain consumer rights and fair commercial practices in the digital environment

References

- European Consumers Organization (BEUC). *Consumer Digital Rights Campaign* [online]. Available from: http://www.consumersdigitalrights.org/cms/index_en.php. [Accessed 9 May 2008].
- European Consumers' Organization BEUC (2006). *Content Online in the Single Market - Public consultation - BEUC response* [online]. Available from: http://ec.europa.eu/comm/avpolicy/docs/other_actions/contributions/beuc_col_en.pdf [Accessed May 9 2008].
- Electronic Privacy Information Center (2004). *Digital Rights Management and Privacy* [online]. Available from http://epic.org/privacy/drm/. [Accessed 9 May 2008].
- Trans Atlantic Consumer Dialogue (2005). *Resolution on Digital Rights Management* [online]. Available from http://www.tacd.org/db_files/files/files-380-filetag.doc. [Accessed 9 May 2008].
- Trans Atlantic Consumer Dialogue (2007). *Transatlantic Consumer Dialogue Recommendations to the Transatlantic Economic Council* [online]. Available from: http://www.tacd.org/db_files/files/files-430-filetag.pdf. [Accessed 19 May 2008].
- Transatlantic Consumer Dialogue (TACD) (2008), *Charter of Consumer Rights in the Digital World*. [online]. Available from: http://www.tacd.org/db_files/files/files-442-filetag.pdf [Accessed 19 May 2008].

3.2 Privacy and Data Protection

One of the greatest challenges for the future of the Internet is the protection of the right of privacy, in particular information privacy. Privacy is a fundamental human right[16]. It underpins

[16] See Universal Declaration of Human Rights (1998). Article 20(1) [online]. Available from: http://www.un.org/Overview/rights.html. [Accessed 9 May 2008].

human dignity and other values such as freedom of association and freedom of speech. Privacy has become one of the most important human rights of the modern age insofar as it might be viewed as a condition for all other liberties[17]. Interest in the right of privacy increased in the 1960s and 1970s with the advent of information technology. The surveillance potential of powerful computer systems prompted demands for specific rules governing the collection and handling of personal information. Two crucial international data protection instruments, the OECD Privacy Guidelines and the Council of Europe's 1981 Convention on Privacy, set out specific rules covering the collection, storage and dissemination of electronic data. These Privacy Guidelines are as relevant in 2008 as they were in 1981, and provide a solid foundation for data protection in global networks. Moreover, nearly all OECD countries include a right of privacy in their Constitution, either directly, in relation to another right or through a Court Decision, and nearly all countries have comprehensive or sectoral privacy laws[18]. However, even in those countries with comprehensive data protection laws, compliance levels appear to be low and enforcement mechanisms weak[19].

Reports of data security breaches in the private and public sectors have become commonplace; online service providers and advertisers are collecting ever-more detailed information about Internet users for their own purposes, and many governments are increasingly accessing databases for law enforcement, national security and other administrative purposes without the limits and public accountability mechanisms that traditionally have safeguarded the right to privacy and the dignity of citizens.

Increasingly sophisticated computer technologies permit the collection, storage, linking, use and sharing of individual data on a scale never before experienced. And market forces drive organizations to take advantage of these opportunities for purposes of profit maximization, cost-effective delivery of services or social control. Moreover, the increasingly global nature of commerce has highlighted challenges raised by trans-border flows of personal information, especially between countries with significantly different domestic data protection regimes.

Personal data collected for a specific purpose by government and private organisations is increasingly being transferred across borders to government agencies for unrelated purposes, often justified on law enforcement or counter-terrorism grounds. These transfers often take place without knowledge or consent, and individuals lose rights of access, correction and challenge.

We recommend that all OECD member countries should:

- adopt comprehensive data protection laws covering both public and private sector use of citizen data, and covering all private and public sector organizations;

[17] Rotenberg, Marc (2000). Preserving Privacy in the Information Society. EPIC [online]. Available from: http://www.unesco.org/webworld/infoethics_2/eng/papers/paper_10.htm. [Accessed 9 May 2008].

[18] Electronic Privacy Information Center and Privacy International (2007). Privacy and Human Rights Report [online]. Available from: http://www.privacyinternational.org. [Accessed 9 May 2008].

[19] See, for example, CIPPIC (2006). *Compliance with Canadian Data Protection Laws; Are Retailers Measuring Up?* [online] Available from: http://www.cippic.ca/documents/bulletins/compliance_report_06-07-06_(color)_(cover-english).pdf. [Accessed 9 May 2008]. See also Greenleaf et al (2007). Promoting and Enforcing Privacy Principles: an analysis of the Australian Privacy Law Reform Commission proposals for the role of the Privacy Commissioner. *Cyberspace Law and Policy Centre* [online]. Available from: http://www.cyberlawcentre.org/ipp/publications/papers/ALRC_DP72_Enforce_final.pdf. [Accessed 9 May 2008].

- ensure such data protection laws should effective enforcement mechanisms so as to promote accountability and compliance;
- fund independent bodies with the mandate to protect privacy, and ensure that such bodies have sufficient resources to oversee privacy laws in both private and public bodies;
- ensure that data protection laws are technology neutral, and that implementation of new technologies, such as RFID, biometrics and GPS applications, complies with existing data protection legislation;
- ensure effective consumer control of personal data, through collection of personal data (including internet usage information and IP addresses) only when strictly necessary and in an open and transparent way, and wherever practicable and lawful, through free, informed and positive consent (opt-in);
- cooperate with each other in respect of cross-border enforcement of privacy protection laws.
- ensure that where personal information is transferred across borders for law enforcement and national security purposes, individuals privacy rights are maintained.

References

- Office of the Privacy Commissioner of Canada (2007). *Declaration of Civil Society Organizations on the Role of Data Protection and Privacy Commissioners* [online]. Canada: Office of the Privacy Commissioner of Canada. Available from: http://www.privcom.gc.ca/information/conf2007/res_ngo_06_e.asp. [Accessed 9 May 2008].
- Privacy International (2006). *Privacy and Human Rights Report 2006*. United Kingdom: Privacy International [online]. Available from: http://www.privacyinternational.org/phr. [Accessed 9 May 2008].
- Transatlantic Consumer Dialogue (2005). *Resolution on Radio-Frequency Identification (RFID)*. United States: Transatlantic Consumer Dialogue [online]. Available from: http://www.tacd.org/cgi-bin/db.cgi?page=view&config=admin/docs.cfg&id=274. [Accessed 9 May 2008].
- Transatlantic Consumer Dialogue (2005). *Resolution on Passenger Name Records.* United States: Transatlantic Consumer Dialogue [online]. Available from: http://www.tacd.org/cgi-bin/db.cgi?page=view&config=admin/docs.cfg&id=254. [Accessed 9 May 2008].

OECD References

- OECD (2007). *Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy* [online]. Available from: http://webdomino1.oecd.org/horizontal/oecdacts.nsf/Display/F3AFC0A8811CEE34C12573C900540EAE?OpenDocument. [Accessed 9 May 2008].
- OECD (1998). *Ministerial Declaration on the Protection of Privacy on Global Networks* [online]. Available from: http://www.oecd.org/dataoecd/39/13/1840065.pdf. [Accessed 9 May 2008].
- OECD (1980). *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* [online]. Available from: http://www.oecd.org/document/18/0,3343,en_2649_201185_1815186_1_1_1_1,00.html. [Accessed 9 May 2008].

- OECD (1985). *Declaration on Trans-border Data Flows* [online]. Available from: http://www.oecd.org/document/60/0,3343,en_2649_201185_2373500_1_1_1_1,00.html. [Accessed 9 May 2008].
- OECD (1997). *Recommendation Concerning Guidelines for Cryptography Policy* [online]. Available from: http://webdomino1.oecd.org/horizontal/oecdacts.nsf/Display/2B230761F2E1A4F7C1257297005E8F46?OpenDocument. [Accessed 9 May 2008].
- OECD (2003). *Privacy Online: Guidance on Policy and Practical* [online]. Available from: http://www.oecd.org/document/49/0,3343,en_2649_201185_19216241_1_1_1_1,00.html. [Accessed 9 May 2008].
- OECD (2006). *Radio-Frequency Identification (RFID): Drivers, Challenges and Public Policy Considerations* [online]. Available from: http://www.oecd.org/dataoecd/57/43/36323191.pdf. [Accessed 9 May 2008].

3.3 Fair Commercial Practices

In 1999, further to the 1998 OECD Ministerial Declaration on Consumer Protection in the Context of Electronic Commerce, the OECD Council issued a Recommendation on Guidelines for Consumer Protection in E-Commerce. Much work has been done by the OECD and member countries to implement these recommendations over the past decade. However, new challenges have arisen, and some pre-existing challenges continue to threaten the future of Internet commerce. The time is ripe for a review of the OECD Consumer Protection Guidelines. These emerging issues are:

3.3.1 Online advertising and behavioral targeting

Consumers have benefited greatly from free online services such as search, news, information sharing and social networking sites. The business model underlying these free services is advertising based on detailed, user-specific information collected as consumers browse, communicate and transact on the Internet. It is explicitly designed to influence consumers, including children, in highly subtle and covert ways by, for example, embedding product endorsements in other, non-commercial communications; blurring distinctions between advertising and editorial contents; exploiting loopholes in existing fair marketing guidelines; and takeovers of home pages or profiles on social networking sites for commercial marketing purposes. Furthermore, increasing vertical consolidation between search engines and online advertising companies give them unprecedented control over huge personal information databases and threaten competition for online marketing business.

Recognizing all this in the context of the Google-Double-Click merger, the U.S. Federal Trade Commission held Town Hall meetings in November 2007 on the issue of "E-havioral Advertising",[20] and later issued for comment a proposed set of "Online Behavioral Advertising Privacy Principles"[21], including that "Every Web site where data is collected for behavioral advertising should provide a clear, consumer-friendly, and prominent statement that data is being

[20] Federal Trade Commission *(2007). ehavioral Advertising – Tracking, Targeting, Technology*. United States: Federal Trade Commission [online]. Available from*:* http://www.ftc.gov/bcp/workshops/ehavioral/index.shtml. [Accessed 9 May 2008].

[21] Federal Trade Commission (2007). *FTC Staff Proposes Behavioral Advertising Privacy Principles*. United States: Federal Trade Commission [online]. Available from: http://www.ftc.gov/opa/2007/12/principles.shtm. [Accessed 9 May 2008].

collected to provide ads targeted to the consumer and give consumers the ability to choose whether or not to have their information collected for such purpose."

We recommended that all OECD member countries should:

- develop new guidelines for online advertising, sales promotions and direct marketing, including to children.
- establish a "Do Not Track" registry, similar to those in some countries preventing telephone cold calling and junk mail.

References

- Center for Democracy and Technology (2003). *A Briefing on Public Policy Issues Affecting Civil Liberties Online from the Center for Democracy and Technology*. United States: Center for Democracy and Technology (CDT) [online]. Available from: http://www.cdt.org/publications/pp_9.13.shtml. [Accessed 9 May 2008].
- Electronic Privacy Information Center (1999*). Online Profiling Project - Comment, P994809 / Docket No. 990811219-9219-01*. United States: Electronic Privacy Information Center [online]. Available from: http://epic.org/privacy/internet/profiling_reply_comment.PDF. [Accessed 9 May 2009].
- Fielder, A et al (2007). Fair Game? Assessing commercial activity on children's favorite websites and online environments. United Kingdom: National Consumer Council [online]. Available from: http://www.ncc.org.uk/nccpdf/poldocs/NCC182rr_fair_game.pdf. [Accessed 9 May 2008].

3.3.2 Unfair e-contracting methods and terms

Many online businesses continue to use contracting methods and to impose terms that are unfair to consumers when purchasing services or virtual copyrighted goods online, such as software, music or books.

Commons unfair practices include:

- not making terms and conditions publicly available for consumers to review prior to purchase;
- not making terms and conditions easily retainable and printable by online consumers;
- binding consumers to terms and conditions without bringing such terms to the consumer's attention ("browse-wrap contracts");
- overly long and complicated terms and conditions, often poorly adapted to the goods or services purchased.

Common unfair terms in electronic contracts include those:

- that give the vendor the right to make material changes to the contract at will without proper notice to the consumer (e.g., by simply posting the updated contract on the vendor's website);
- that purport to limit the vendor's liability unreasonably;
- that shift legal uncertainties onto the consumer when laws vary between countries;
- that prohibit consumers from making otherwise legal uses of products and services purchased or from criticizing the vendor; and

- that deny consumers the right to class actions or other court actions in the case of disputes.

Many of these unfair terms and practices are recognized as such in European law and are treated as unenforceable in law (although end-user licences for digital products are currently exempt from some European consumer protection laws). North American law, however, tends to apply the much higher standard of "unconscionability" and in so doing permits unfair practices such as those listed above. Allowing e-businesses to impose unfair terms on consumers or to engage in unfair practices undermines consumer confidence in e-commerce.

We recommend that all OECD member countries should:

- prohibit or, at a minimum legislate the invalidity of unfair terms in consumer contracts.
- legislate the invalidity of online contractual terms that disadvantage consumers where such terms were not made publicly available, were not explicitly agreed to by the consumer, or could not be easily saved and printed by online consumers.
- extend the scope of basic consumer protection legislation, such as guarantees and rights of return, to include digitally downloaded goods (music, software).

References

- Belgrove, C. (2008). *Whose license is it anyway? A study of end-user license agreements for computer software*. United Kingdom: National Consumer Council [online]. Available from: http://www.ncc.org.uk/nccpdf/poldocs/NCC195rr_whose_licence.pdf. [Accessed 9 May 2008].
- National Consumer Council (2007). *European Consumer Law - Responses to the European Commissions Green Paper on the review of the consumer acqui*s [online]. Available from: http://www.ncc.org.uk/nccpdf/poldocs/NCC157cr_acquis_response.pdf. [Accessed May 18, 2008].

OECD Documents

- OECD. *Guidelines for Consumer Protection in the Context of Electronic* Commerce [online]. Available from: http://www.oecd.org/dataoecd/18/13/34023235.pdf. [Accessed 9 May 2008].

3.3.3 Mobile Commerce

Mobile commerce is an increasingly widespread business model that enables consumers to purchase goods and services using mobile phones or other devices with access to mobile networks. While mobile commerce can provide great convenience, it can also pose certain risks that should be addressed now while still in the early stages of development. Downloading ring tones and screen savers are the most common types of purchases via mobile phones, but other service and product provision is on the increase, such as polling, chat lines, games, ticket purchases or weather forecasts. Charges may appear on the mobile service bill, or be billed to a credit card or bank account. Mobile devices in themselves are becoming payment instruments, if for example equipped with RFID.

Consumer complaints and concerns about unfair business practices and fraudulent activities in connection with mobile commerce are increasing. A survey of consumers conducted by TACD in 2006 showed that 38% of respondents had problems related to mobile commerce; misleading

representations regarding the costs of goods and services was the most frequent problem cited. Even more significant, the majority of those who had problems did not complain, and half of those who tried to resolve their problem were unsuccessful.

Other issues linked to mobile commerce include inadequate protections against unauthorised charges; marketing targeted at children and adolescents who may have no capacity or authorization to make purchases; inadequate disclosures about products and services offered and terms and conditions; and spam over mobile phones. Furthermore, since laws may differ from country to country, it is difficult for consumers to know what their rights are as they travel and use mobile commerce, and for law enforcement agencies to take effective cross-border action.

We recommend that all OECD member countries should:

- assess whether existing OECD countries laws and regulations apply to mobile commerce, identify gaps and inconsistencies;
- study the impact of mobile commerce on vulnerable and disadvantaged consumers, such as children and those on low income;
- ensure that existing consumer protection regulations and self-regulatory codes of practice are technology neutral and include commercial transactions over mobile phones;
- ensure that consumers using mobile devices to transact are protected against unauthorized transactions, misleading marketing practices, spam and unsolicited advertisements; and have specific rights to terminate on short notice subscriptions to premium content and services;
- ensure effective redress mechanisms for consumer disputes regarding mobile commerce.

References

- Transatlantic Consumer Dialogue (2005*). Resolution on Mobile Commerce, Infosoc-32-05*. United States: Transatlantic Consumer Dialogue [online]. Available from: http://wwwtacd.org. [Accessed 9 May 2008].
- Transatlantic Consumer Dialogue (2006*). Report on the July 2006 TACD Mobile Commerce Survey* [online]. Available from: http://www.tacd.org/db_files/files/files-413-filetag.pdf. [Accessed 9 May 2008].

3.3.4 Unsolicited Commercial Email: Spam

Spam (unsolicited bulk email) now accounts for the vast majority of email traffic on the Internet. In addition to being a nuisance, important messages are lost in the flood of spam or captured by spam filtering tools, and costs of spam filtering by ISPs are ultimately paid by consumers. The general base of Internet users also ultimately pays for the overall bandwidth used by spam. Finally, spam is often a vehicle for malware or deceptive business practices, such as "phishing" scams and sales of counterfeit medicine. These combined effects of spam have reduced the reliability of email as a means of communication and are thus threatening the viability of e-commerce.

A survey conducted by the TACD in late 2003 shows that concern about unsolicited commercial electronic messages clearly has a negative impact on the growth of e-commerce. Fifty-two percent of respondents said that they shop online less or not at all because they are worried about

receiving such messages[22]. Some bodies do not accept official communications by email, presumably because of its unreliability caused in part by the preponderance of spam[23].

Many OECD member governments have passed anti-spam legislation,[24] and industry stakeholders have made significant strides in containing the problem through self-regulation. Nevertheless, spam continues to pose a significant threat to the viability of email as a commercial medium of communication.

We recommend that all OECD member countries should:

- ensure proper enforcement of existing anti-spam legislation, with effective penalties for non-compliance;
- where applicable, establish laws outlawing spam and procedures for holding spammers accountable;
- redouble cooperative efforts to address cross-border aspects of the problem.

References

- Transatlantic Consumer Dialogue (2005*). Resolution on unsolicited commercial email (Internet-29-04)* [online]. Available from: http://www.tacd.org/cgi-bin/db.cgi?page=view&config=admin/docs.cfg&id=224. [Accessed 9 May 2008].
- Center for Democracy and Technology (2004). Spam Continues to Plague Industry and Users (Policy Post 10.15). United States: Center for Democracy and Technology (CDT) [online]. Available from: http://www.cdt.org/publications/pp_10.15.shtml. [Accessed 9 May 2008].

OECD Documents

- OECD (2006). *Recommendation on Cross-Border Co-operation in the Enforcement of Laws against Spam* [online]. Available from: http://www.oecd-antispam.org/article.php3?id_article=237. [Accessed 9 May 2008].
- OECD (2006). *Anti-Spam Toolkit and Annexes* [online]. Available from: http://www.oecd-antispam.org/article.php3?id_article=265. [Accessed 9 May 2008].
- Federal Trade Commission (2004). *London Action Plan on International Spam Enforcemen*t. United States: Federal Trade Commission [online]. Available from: http://www.ftc.gov/os/2004/10/041012londonactionplan.pdf. [Accessed 9 May 2008].

3.3.5 Cross-border dispute resolution

As already noted, cross-border online retail commerce has grown more slowly than many predicted in 1998. A significant disincentive to cross-border shopping by consumers is the risk of being unable to obtain redress should something go wrong with the transaction. Consumers are

[22] Message Labs Intelligence (2008). *Monthly Reports from OECD's Task Force on Spam's Statistics and Data section of their website* [online]. Available from: http://www.messagelabs.com/intelligence.aspx. [Accessed 9 May 2008].

[23] E.g., Office of the Privacy Commissioner of Canada, Online organizations typically require consumers to use webforms, as opposed to email, in order to communicate electronically. Such forms are problematic insofar as they do not automatically leave consumers with a record of the communication.

[24] Countries with anti-spam legislation include Argentina, Australia, Japan, New Zealand, Russia, South Korea, U.S.A. and all EU member countries.

much more likely to engage in cross-border e-commerce if they are assured that, should a dispute arise, they can obtain redress via the relevant tribunals or courts of their own jurisdiction, and that they are protected by the laws of their jurisdiction.

The OECD and its member countries have done much work since 1998 on developing effective online dispute resolution mechanisms so as to facilitate e-commerce. However, effective dispute resolution options that are low cost, independent and fair for consumers remain limited. Online vendors continue to include "mandatory arbitration" clauses in their contracts of sale or service, requiring that consumers submit any dispute that arises to private arbitration rather than to court. A primary purpose of such clauses is to avoid class actions by consumers. A number of jurisdictions have made such clauses unenforceable in law, but many OECD member countries have not done so.

Also common in online contracts are clauses establishing that all disputes must be resolved in the courts of a specified jurisdiction under the laws of that jurisdiction. Such jurisdiction may be that of the vendor, or another locale (in which, for example, the vendor enjoys more rights vis-à-vis the consumer). Again, some jurisdictions have legislated their citizens' right to access local courts and apply local consumer protection laws[25], but this is not the case everywhere.

Consumers should have greater choice with respect to dispute resolution options, especially in the online and cross-border contexts.

We recommend that OECD member countries should:

- invalidate mandatory arbitration clauses in pre-dispute consumer contracts through legislation;
- override choice of law and forum clauses that deprive consumers of their right to access local courts under local laws where the business knowingly advertised or sold to the consumer's jurisdiction;
- continue to explore and support effective online dispute resolution options for consumers.

References:

- Transatlantic Consumer Dialogue (2002). *Resolution on Jurisdiction in Cross-Border Consumer Contracts* [online]. Available from: http://www.tacd.org/cgi-bin/db.cgi?page=view&config=admin/docs.cfg&id=44. [Accessed 9 May 2008].
- Transatlantic Consumer Dialogue (2002). *Resolution on ADR in the Context of Electronic Commerce* [online]. Available from: http://www.tacd.org/cgi-bin/db.cgi?page=view&config=admin/docs.cfg&id=41 . [Accessed 9 May 2008].
- Consumers International (2001). *Disputes in Cyberspace 2001: Update of Online Dispute Resolution for Consumers in Cross-border Disputes* [online]. Available from: http://www.consumersinternational.org/Shared_ASP_Files/UploadedFiles/DD330597-5945-4B5A-A8BD-4A6573F3F9AF_ADRReport2001.pdf. [Accessed 9 May 2008].

[25] Brussels Convention on: Court of Justice of the European Communities (2007). *Convention of the Jurisdiction and the enforcement of Judgements in civil and commercial matters* [online]. Available from: http://curia.europa.eu/common/recdoc/convention/en/c-textes/brux-idx.htm. [Accessed 9 May 2008]. See: Rome-convention.org (2002). *Convention on the Law applicable to contractual obligations opened for signature in Rome on 19 June 1980* [online]. Available from: http://www.rome-convention.org/instruments/i_conv_orig_en.htm. [Accessed 9 May 2008].

OECD Documents

- OECD (2007). *Recommendation on Consumer Dispute Resolution and Redress* [online]. Available from: http://www.oecd.org/document/45/0,3343,en_2649_201185_38967917_1_1_1_1,00.htm. [Accessed 9 May 2008].
- OECD (2005). *OECD Workshop on Consumer Dispute Resolution and Redress in the Global Marketplace* (19-20 April 2005) Background Report [online]. Available from: http://www.oecd.org/dataoecd/59/21/34699496.pdf. [Accessed 9 May 2008].

3.4 Identity Management and Reputation

Systems for electronic identification and authentication have been in place in a number of countries for a few years now, and experience shows a strong link between privacy and identity issues. The failure of large-scale single sign-on services has shown that citizens and customers are only accepting identification technologies if their privacy is fully respected. The 2006 OECD Guidance on Electronic Authentication includes the principles of proportionality and privacy. While this is a good first step, new technology allows for greater security while maintaining individual anonymity. Such systems should be encouraged. Important elements include:

Minimal disclosure: Identity and authentication systems must only provide the information that is needed for the actual transaction. For this, full anonymity must be the default option, and single information bits are then added consciously and sparingly. Regulation must ensure that data is not collected if it is not needed for the service in case.

Non-Linkability: Digital identifiers have to be constructed in a way that they can not be linked across contexts and transactions, and allow context-sensitive pseudonyms. This will protect users from profiling and at the same time significantly shield against identity theft.

Non-Traceability: Increasingly, online authentication towards third parties (like business and government agencies) is done by identity providers. Identification systems that are based on this model must ensure that the identity provider can not trace and track the services the user has used.

User Control: All identifying information about an individual must flow through the individual's hands, and it must be readable by the individual. This concept of "user-centric identity" must become the basis for general identification and authentication systems in the public and private sector.

Application to Government-issued Identity Tokens: The above-mentioned principles are especially relevant when moving towards government-issued identity tokens. Additionally, legislation must ensure that citizens can still use paper-based documents.

Relationship Information Belongs to Both Parties: Social networking platforms have to take into account that information about a relationship belongs to both parties. Therefore, services allowing users to publish information about others as well as about relationships have to ensure this can only be done when both parties have agreed to it under the same conditions.

Identity systems designed with these principles in mind can ensure user privacy as well as security, and also offer protection against the growing problem of identity theft[26]. In the offline world, we can show an ID card or a drivers' license without the issuing agency knowing about this. The same amount of privacy has to be built into online identity systems. The basis for all this is the possibility to have full online anonymity in the first place. Attempts to prohibit online anonymity by law are not compatible with our understanding of a free society.

Reputation and rating systems add another important layer of concern to identity management systems. Increasingly, services generate aggregated ratings of individuals based on the mass input by other users, be it in online auctions and warehouses, in schools and universities, and elsewhere. Users must only become subject to this if they consciously agree, and they must have easy access to mechanisms of redress when rated maliciously or openly false. Additionally, it must be ensured that the reputation data is only used in the context it was generated for, and that individuals are not made the subjects of purely automated decisions that affect their life chances. The latter principle is already incorporated in the EU Data Protection Directive of 1995. Services allowing users to publish information about others as well as about their relationships have to ensure this can only be done when both parties have agreed to it under the same conditions.

We recommended that OECD member countries should:

- actively engage in informing society about the dimensions of digital identity solutions.
- implement the OECD Recommendation on Electronic Authentication.
- encourage the development and deployment of IDM systems that fully adhere to the principles of user control and user-centricity.
- encourage research and knowledge transfer about these identity solutions.
- investigate what kind of redress processes individuals should have at their disposal for information about them.
- enact legislation that offers reasonable, effective and inexpensive means of redress for individuals whose reputation is endangered by rating and reputation systems.
- enact strict limits on private sector use of government identification numbers.

References:

- Kim Cameron's Identity Weblog (2005). Introduction to the Laws of Identity [online]. Available from: http://www.identityblog.com/?p=354. [Accessed 9 May 2008].
- Cavoukian, A. (2006.) *7 Laws of Identity The Case for Privacy-Embedded Laws of Identity in the Digital Age* [online]. Canada: Information and Privacy Commissioner of Ontario. Available from: http://www.ipc.on.ca/images/Resources/up-7laws_whitepaper.pdf. [Accessed 9 May 2008].
- Privacy and Identity Management for Europe. (2008). *PRIME Principles* [online]. Available from: https://www.prime-project.eu/about/principles/. [Accessed 9 May 2008].
- Privacy and Identity Management for Europe. (2007). *PRIME White Paper* [online]. Available from: https://www.prime-project.eu/prime_products/whitepaper/. [Accessed 9 May 2008].

[26] According to the US Federal Trade Commission, for the seventh year in a row, identity theft is the number one consumer complaint category. See US Federal Trade Commission (2008*) Consumer Fraud and Identity Theft Complaint Data Full Report* [online]. Available from: http://www.ftc.gov/opa/2008/02/fraud.pdf [Accessed 18 May 2008].

- Identity Commons. (2008). *Identity Rights Agreement* [online]. Available from: http://wiki.idcommons.net/index.php/Identity_Rights_Agreements. [Accessed 9 May 2008].
- Open Social Web (2007). *A Bill of Rights for Users of the Social Web* [online]. Available from: http://opensocialweb.org/2007/09/05/bill-of-rights/. [Accessed 9 May 2008]

OECD References:

- OECD (1998). *Ministerial Declaration on Authentication for Electronic Commerce*. [online]. Available from: http://www.olis.oecd.org/olis/1998doc.nsf/linkto/dsti-iccp-reg(98)9-final [Accessed 19 May 2008].
- OECD. (2007). OECD *Recommendation on Electronic Authentication and Guidance for Electronic authentication* [online]. Available from: http://www.oecd.org/document/7/0,3343,en_2649_33703_38909639_1_1_1_1,00.html. [Accessed 9 May 2008].
- OECD Directorate for Science, Technology and Industry. (2007). At a Crossroads: "Personhood" and Digital Identity in the Information Society (STI Working Paper 2007/7) [online]. Available from: http://www.oecd.org/LongAbstract/0,3425,en_2649_201185_40204774_119684_1_1_1, 00.html. [Accessed 9 May 2008].

3.5 Network Security and Prevention of Fraud

Possibly the greatest impediment to consumer e-commerce is lack of security on the Internet. Insecure practices by e-commerce providers can have severe consequences for consumers, such as damage to their computers and their contents, theft of their data for fraudulent purposes and intrusive marketing. Examples of digital products and services that are not sufficiently safe include websites, wireless modems, personal computers sold without any security features, and insecure payment systems. In addition consumers are not professionally trained to deal with this problem and protections are hard to keep up-to-date as the Internet is a dynamic environment – criminal attacks in general are relatively easy, quickly executed and difficult to detect or trace.

A recent US Consumer Reports survey showed that consumers in the US paid $7.8 billion over two years to repair or replace computers infected with viruses and spyware. A similar survey in the Netherlands found that 62% of Dutch PC users were confronted with problems like spam, spyware or viruses during 2006. Other research shows that security suites do not live up to consumer expectations. The main responsibility for protection against threats and attacks to digital security is placed on end users, but improving security in digital environments is an issue that involves many parties, including but not limited to consumers. At the same time there is a growing number of identity theft (ID theft) and other attacks, such as phishing, pharming and spoofing via the Internet. Consumer confidence is at stake, as trust in doing business online is eroded due to the increasing risk of such attacks. Surveys show that consumers change their online behavior, or are reluctant to start transacting online due to fears of identity theft, while recent reports show that victims of identity theft can suffer from stress and health problems while fighting to rehabilitate their identities. Current efforts by authorities to combat these crimes are not sufficient, especially when it comes to more sophisticated or high-tech forms of attack. Many OECD countries do not even have specific offenses covering identity theft, which is often erroneously considered a victimless crime.

We recommend that OECD member countries should:

- Enact laws to explicitly prohibit the use of malware and spyware, as well as remote manipulation of external computers and services for deceptive or fraudulent purposes.
- Require the providers of electronic products and services to safeguard their security and make them legally accountable for losses and damage caused by not taking appropriate security measures.
- Establish effective enforcement measures to prevent large-scale economic damages as a result of security breaches.
- Update national laws to address ID theft holistically, including: general duties on companies and governments to adopt adequate security policies and procedures and to inform customers when their data has been compromised (security breach legislation); and provisions to enable consumers to places 'freezes' on their credit reports.
- Create dedicated centers to help victims of ID theft repair their financial affairs, including dedicated help-lines and international hot lines.

References

- Transatlantic Consumer Dialogue. (2002). *Resolution on Protecting Consumers from Fraud and Serious Deception Across Borders* [online]. Available from: http://www.tacd.org/cgi-bin/db.cgi?page=view&config=admin/docs.cfg&id=179. [Accessed 9 May 2008].
- Transatlantic Consumer Dialogue. (2007). *Resolution on Internet Security* [online]. Available from: http://www.tacd.org/db_files/files/files-418-filetag.pdf. [Accessed 9 May 2008].
- Transatlantic Consumer Dialogue. (2007). *Resolution on Identity Theft, Phising and Consumer Confidence* [online]. Available from: http://www.tacd.org/docs/?id=306. [Accessed 9 May 2008].
- US Consumers Union. (2004). *Identity Theft: Action and Prevention for Consumers* [online]. Available from: http://www.consumersunion.org/finance/id-theft03.htm. [Accessed 9 May 2008].
- National Consumer Council. (2006). *Identity Theft Victim Support National Consumer Council Blueprint for Action* [online]. Available from: http://www.ncc.org.uk/nccpdf/poldocs/NCC128a_br_ID_theft.pdf. [Accessed 9 May 2008].
- Fox, Susannah. (2005). *Spyware: The Threat of Unwanted Software Programs is Changing the Way People Use the Internet* [online]. Washington, D.C., United States: Pew Internet & American Life Project. Available from: http://www.pewinternet.org/PPF/r/160/report_display.asp. [Accessed 9 May 2008].

OECD Documents

- OECD. (2003). OECD *Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders* [online]. Available from: http://www.oecd.org/document/50/0,3343,en_2649_201185_2514994_1_1_1_1,00.html. [Accessed 9 May 2008].

4.0 Benefiting from convergence

Increasingly, the various networks and modes of communication that connect individuals are themselves becoming interconnected. This communications convergence promises significant

benefits to many aspects of society, allowing for social, political, cultural, and economic exchange with unprecedented speed and ubiquity. Ensuring that the public benefits from these technological advances requires that information flow freely and easily among various networks, protocols, applications, and devices.

To enable such interoperability while preserving a competitive and democratic environment, member countries must support the implementation of open standards and promote nondiscriminatory, neutral networks.

4.1 Interoperability and open standards

In order to achieve the interoperability necessary for convergence, hardware and software must use sets of common standards. Using open standards allows us to reap the full social and competitive benefits of convergence, by allowing for robust competition, promoting social and governmental transparency, and facilitating digital archiving.

As paragraph 44 of the WSIS Declaration of Principles states:

"Standardization is one of the essential building blocks of the Information Society. There should be particular emphasis on the development and adoption of international standards. The development and use of open, interoperable, non-discriminatory and demand-driven standards that take into account needs of users and consumers is a basic element for the development and greater diffusion of ICTs and more affordable access to them, particularly in developing countries. International standards aim to create an environment where consumers can access services worldwide regardless of underlying technology"[27].

The success and flexibility of this model has been demonstrated by the rapid growth of the Internet and the Web, based upon standards that were freely accessible to the public and to developers. As different types of technology begin to interact with the Internet, it is crucial that this same adaptability expand with it.

Because it was based on open technical standards, the Internet expanded far beyond its original design to exploit new information technologies, new business models for investment, and new social models for governance.

The methods of communication that were at the core of the Internet were those that focused on the needs and values of the users, particularly when sharing information. The focus was on an ever-expanding toolkit of methods for finding, disseminating and presenting information, and increasingly on gathering and creating valuable data and works of commentary and analysis. The commitment to open standards was an early and durable feature of the network development, always in tension with the efforts by firms to introduce or impose proprietary technologies.

The relationship between free and open standards and proprietary technologies continues to present tensions, but both have played an important role. The existence of core technologies that

[27] World Summit on the Information Society. (2003). Document WSIS-03/GENEVA/DOC/4-E. *Proceedings from the Declaration of Principles- Building the Information Society: a global challenge in the new Millennium* [online]. Geneva: WSIS. Available from: http://www.itu.int/wsis/docs/geneva/official/dop.html. [Accessed 22 May 2008].

are both free and open have protected the network from monopolization, while not interfering in the serial introductions of new commercially motivated products and services, that alternatively compete and cooperate with other free and non-free technologies.

One of the clear benefits of open standards is that they allow for full and healthy competition even in situations where network effects tend to create a natural monopoly in the particular technology[28]. Open standards help to ensure that a wide range of different technologies can make use of a standard by eliminating barriers to entry that might otherwise be created by incumbents or more powerful competitors. For example, the open document formats for HTML have led to an explosion of innovation in authoring tools for web pages, in contrast to the highly monopolistic, expensive and non-innovative state of authoring tools for word processing and presentation graphics. By allowing easier entry into networked technological markets, open standards can reduce the likelihood of standards and technical specifications being used to seek monopoly rents from new competitors and innovators. Although interoperability alone can be achieved with standards that are subject to royalties and licensing restrictions, such policies prevent smaller firms or groups of individuals from participating in the market. This can lead to anti-competitive lock-ins as technologies evolve and require upgrading.

Of particular concern are the issues concerning disclosure of assertions of patent rights in connection with proposed standards. At present, these policies are largely regulated by standards making bodies, but only insofar as they apply to members of the standards organization, or, even more limiting, to those members participating in the standards negotiations. In cases where disclosures were said to be lacking, the U.S competition authorities have sought both remunerative and non-remunerative compulsory licenses on the patents, as a remedy to an anticompetitive or unfair practice. There is concern that the voluntary disclosures managed by standards-making bodies are not enough.

In a 2005 drafting exercise, a coalition of WIPO country negotiators, technology firms, academic experts and public and consumer interest NGOs proposed to create a global system for disclosure, that extended beyond the members of the standards organization, in cases involving "open" standards. In Part 6 of the May 9, 2005 draft of a proposed Treaty on Access to Knowledge, a global system for noticing proposed standards would trigger an obligation for any patent owners to disclose patent claims relevant to that standard. Most importantly, the signatory countries to the treaty would agree "a patent holder that fails to make constructive disclosures of relevant patent claims will be prevented from enforcing the patent against the implementation of the open standard."[29]

The May 9, 2005 draft Treaty on Access to Knowledge also proposed other steps to promote the use of open standards, particularly as they related to "Essential Interfaces for Knowledge Goods." For example, the treaty Members would agree, "to consider procurement policies that provide preferences or requirements that computer software, hardware, or accessories that use and enable open, standards compliant interfaces." And, in an approach similar to but more attractive than "license of right" policies in some countries, patents licensed on a non-discriminatory and royalty free basis for use in implementing an interface for an essential knowledge good, "shall not be

[28] Ghosh, Rishab A. (2005). *An Economic Basis for Standards* [online]. Maastricht, the Netherlands: University of Maastricht and FLOSSPOLS. Available from: http://www.intgovforum.org/Substantive_1st_IGF/openstandards-IGF.pdf. [Accessed 22 May 2008].

[29] See Treaty On Access to Knowledge. *Draft 9 May 2005* [online]. Available from: http://www.cptech.org/a2k/a2k_treaty_may9.pdf. [Accessed 22 May 2008].

subject to further fees." Finally, "Members agree to develop procedures for compulsory licensing of essential interfaces for knowledge goods.[30]"

Open standards also provide clear social and democratic advantages when implemented by governments. This highlights the importance of open standards within government procurement policies[31]. In situations where ICT is critical to political processes, transparency is necessary to maintain trust in the legitimacy of the process. For example, voters must be able to assure themselves that machine-tabulated votes are honestly and accurately counted.

Even in conditions of less intense numeric scrutiny, open standards are essential for the public to maintain access to government and social resources through technological means. For instance, public information distributed in closed or proprietary formats can easily reduce the number of citizens with electronic access to critical information. Open formats for electronic forms would also guarantee that the public does not have to rely upon specific application vendors in order to interface with government electronically. Open standards for such information and its transmission ensure that public participation will not be a function of citizens' having access to one particular manufacturer's technology.

The benefits of open standards are also evident in the context of archiving records. As technologies and formats evolve, there is always the possibility of document formats and software applications becoming obsolete. Where those formats are closed, agencies and the public could be prevented from accessing electronic public records. Maintaining records in open formats allows later developers to build software that is backwards-compatible. This issue grows in importance as more and more records are stored and accessed electronically.

We recommend that OECD member countries should:

- Promote a definition of open standards that supports economic and social development goals. Such a definition would specify that open standards:
  - are developed and managed through a collaborative and democratic process;
  - are freely accessible to the public;
  - are free of royalties and other intellectual property constraints;
  - provide irrevocable licenses to use intellectual property that might be infringed in implementation;
  - do not include proprietary “hooks” that create technical or economic barriers;
  - allow multiple, competing implementations to be verified against the standard.

- Encourage adoption of open standards according to the above definition.
- Encourage the creation and adoption of non-proprietary, non-discriminatory hardware and software interfaces through a combination of policy, legislation, regulation, and procurement policies in addition to voluntary standards development actions.
- Ensure that public government services and data are based on open ICT standards.
- Ensure that government procurement policies do not require compatibility with proprietary technologies or proprietary ICT standards.

[30] *Ibid*.

[31] This is a Yale ISP White Paper please see DeNardis, L. and Tam, Eric.[2007]. *Open Documents and Democracy – A Political Basis for Open Document Standards* [online]. United States: Yale Information Society Project. Available from: http://isp.law.yale.edu/static/papers/Open_Documents_and_Democracy.pdf . [Accessed 9 May 2008].

References

- Dynamic Coalition on Open Standards (DCOS). [2006]. *Open ICT Standards Statement* [online]. Available from: http://igf-dcos.org/wp-content/uploads/igf-general-statement-2006.odt. [Accessed 22 May 2008].
- Dynamic Coalition on Open Standards (DCOS). [2006]. *Draft Principles for Open Standards* [online]. Available from: http://igf-dcos.org/wp-content/uploads/dcos-draft-open-standard-principles.odt. [Accessed 22 May 2008].
- Treaty on Access to Knowledge. [2007]. *Draft 9 May 2005* [online]. Available from: http://www.cptech.org/a2k/a2k_treaty_may9.pdf. [Accessed 22 May 2008].

4.2 Open broadband networks and net neutrality

As Internet protocol increasingly becomes the mode of choice for communications, the importance of the Internet has increased, with voice, video, and audio media joining data on packet-switched networks.

Because of this, Internet service providers and communications network providers are increasingly becoming a primary gateway to information for the public. With this increase, however, come more examples of service providers attempting to become not just gateways, but gatekeepers to information, able to block or degrade signals and information that are counter to their interests.

For instance, service providers in Europe, Korea, Mexico, and the United States have all attempted to block voice over IP transmissions from their network, hampering a technological innovation that competed with their own services[32]. In Canada, an ISP prevented its users from reaching the website of a labor union that represented the company's striking employees[33]. In other cases, particular applications or viewpoints have been singled out for discrimination by providers[34].

Network providers should not be allowed to use their control of the networks to discriminate against legitimate traffic for anticompetitive purposes, or for the purposes of interfering with the freedom of opinion and expression. By blocking certain applications or services from

[32] See Charny, B. (2005). *VoIP Backlash in Germany?* [online]. Available from: ZDNet News http://news.zdnet.com/2100-1035_22-5786976.html. [Accessed 9 May 2008]; See also Flack, T.D. (2006). *South Korea Temporarily Lifts Decision to Block VoIP Service* [online]. Available from: (Stars and Stripes) http://www.stripes.com/article.asp?section=104&article=37448&archive=true. [Accessed 9 May 2008]. Another one from Charny, B.(2005). *VoIP Finds Foreign Friends and Adversaries* [online]. Available from: (ZDNet News) http://news.zdnet.com/2100-6005_22-5709459.html. [Accessed 9 May 2008]. Lawson, Steven. (2008). *Vonage CEO Slams VoIP Blocking* [online]. Available from: (PC World) http://pcworld.about.com/news/Mar082005id119919.htm . [Accessed 9 May 2008].

[33] See Geist, M. (2005). *Telus Breaks Net Providers Cardinal Rule* [online]. Available from: http://www.michaelgeist.ca/index.php?option=content&task=view&id=919 . [Accessed 9 May 2008].

[34] Liptak, A. (2007). Verizon Blocks Messages of Abortion Rights Group. *Times* [New York] [online] 27 September 2007. Available from: http://www.nytimes.com/2007/09/27/us/27verizon.html. [Accessed 9 May 2008].

communications networks, discriminating service providers can lock consumers into an anticompetitive environment that stifles technological growth and can stymie the benefits of continuing convergence. By suppressing particular speakers, viewpoints, or types of content, discriminating service providers can exercise undue influence on political and social processes, denying users the benefits of trusted, unfettered communication.

While providers require the ability to manage traffic on their networks in order to ensure quality of service, reasonable management should not include, and does not require, discriminatory and anticompetitive behavior. Legitimate network management may take the form of blocking content harmful to the network, such as viruses and denial of service attacks, or of recognizing different priorities for different types of applications, without discriminating as to provider, sender, or recipient. Legitimate network management would also include compliance with the requirements of local law, or compliance with the express wishes of the affected customer.

Because of the difficulty for ordinary users to determine if delays or blockages are the result of discrimination, network providers should maintain minimum levels of transparency with regard to any traffic management or prioritization they implement. Without such transparency, it would be difficult for regulators to take appropriate action in response to discriminatory or anti-competitive behavior.

We recommend that OECD should:

Develop and promote a standard for network neutrality, defined as a state in which

Consumers have the right:

- to attach devices of their choice.
- to access or provide content, services, and applications of their choice.
- for their access to be free from discrimination according to source, destination, or content.

and in which network providers:

- do not block any lawful content, applications, or devices.
- do not deliberately degrade content or applications.
- do not prioritize data according to its source or destination.
- do not discriminate against particular providers of content, applications, services, or devices.
- do not engage in anticompetitive discrimination.

We recommend that OECD should:

- Develop guidelines for policies that will encourage neutral networks.
- Develop guidelines for provider transparency in network management.

We recommend that OECD member countries should:

- Ensure that network providers do not block, degrade, or discriminate against particular providers of content, applications, services, or devices.
- Ensure that network providers do not engage in anticompetitive discrimination.

- Require network providers to disclose any prioritization or network management on their networks, and ensure that such management is only undertaken for the above-listed legitimate network management purposes.
- Regularly test networks for blocking, degradation, or other discriminatory action.
- Regularly assess disclosed network management to ensure that it is legitimate.
- Provide a means of complaint and redress for users against providers who fail to provide adequate information or engage in unfair discrimination.

References:

- Mueller, M. (2007). *Net Neutrality as a Global Principle for Internet Governance* [online]. United States: Internet Governance Project. Available from: http://www.internetgovernance.org/pdf/NetNeutralityGlobalPrinciple.pdf. [Accessed 9 May 2008].
- Windhausen, John Jr. (2006). *Good Fences Make Bad Broadband: Preserving an Open Internet Through Net Neutrality* [online]. United States: Public Knowledge. Available from: http://www.publicknowledge.org/pdf/pk-net-neutrality-whitep-20060206.pdf. [Accessed 9 May 2008].
- Wu, Tim. (2003). *Network Neutrality, Broadband Discrimination* [online]. United States: Columbia University – Columbia Law School. Available from: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=388863. [Accessed 9 May 2008].
- Transatlantic Consumer Dialogue. (2008). *Resolution on Net Neutrality* [online]. Available from: http://www.publicknowledge.org/pdf/tacd-nn-resolution-200803.pdf. [Accessed 9 May 2008].