

## **EXECUTIVE SUMMARY**

### **The Future of the Internet Economy 'Fueling Creativity, Ensuring Consumer and Privacy Protection and Building Confidence, and Benefiting from Convergence'**

#### **Background**

We as Civil Society reconfirm "our commitment to build a people-centred, 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." as stated in the Geneva Declaration of Principles of the World Summit on the Information Society.

We further confirm our agreement with the European Council to the Internet Governance Forum's emphasis on the 'public service value' of the Internet and its relationship to the achievement of democratic citizenship including "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..."

We see and would expect democratic governments to see the Internet not only as the underpinnings of new market structures, but also as a critical social infrastructure, a necessary element and enabler of the range of classical and contemporary rights and entitlements which underpin the modern state. The emerging Information Economy and Society has new key infrastructural elements at many levels whose 'public nature' needs to be

recognized, and the financing and regulation of these elements in support of the broader public interest has to proceed from this recognition.

To assure equity of access and opportunity for effective use of the Internet for economic as well as other purposes by all in society public investments will be needed as a matter of social policy, to respond to the variety of basic needs and rights of citizens and others and to address various social inclusions.

Action:

Governments acknowledge and support in their policy, programmes 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.

## **1.0 Fundamental Policy Principles**

It is vitally important now and into the future of the Internet Economy, that the Internet is founded on respect for fundamental human rights and freedoms, democracy, the rule of law, and sustainable development. Governments have a duty to uphold and respect human rights, individual privacy, freedom of expression and opinion, access to knowledge and the public domain, cultural diversity; and to correct market failures; protect citizens from unfair and deceptive business practices; to ensure widespread access to the Internet through, as required, publicly supported public and community based Internet Access points; and to recognize the role that the Internet is playing as a critical social infrastructure by ensuring that it is universally accessible and usable by all.

In the OECD Ministerial Framework, Civil Society reconfirms "our commitment to build a people-centred, 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<sup>1</sup>" as stated in the Geneva Declaration of Principles of the World Summit on the Information Society.

Civil Society further confirms our agreement with the European Council to the Internet Governance Forum's emphasis on the 'public service value' of the Internet and its relationship to the achievement of democratic citizenship including "that everyone should be entitled to expect the delivery of a

---

<sup>1</sup> See WSIS, Declaration of Principles: Building the Information Society: a global challenge in the new Millennium, available at <<http://www.itu.int/wsis/docs/geneva/official/dop.html>>.

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.

Civil Society sees and expect democratic governments to see the Internet not only as the underpinnings of new market structures, but also as a critical social infrastructure, a necessary element and enabler of the range of classical and contemporary rights and entitlements which underpin the modern state. The emerging Information Economy and Society has new key infrastructural elements whose 'public' nature needs to be recognized. CS believes that in support of the broader public interest the financing and regulation of these elements has to proceed from this recognition.

To assure equity of access and opportunity for effective use of the Internet for economic as well as other purposes by all in society, public investments will be needed as a matter of social policy, to respond to the variety of basic needs and rights of citizens and others and to ensure the broadest possible degree of social inclusion.

- The 2008 OECD Ministerial will be an opportunity for the OECD to reaffirm its "commitment to safeguarding important human rights and prerogatives in an Age of Global Digital Networks, by formulating baseline principles that safeguard individuals' rights and the confidence that commerce and communities demand; guide governments in articulating forward-looking public policy, and encourage all stakeholders in developing social, cultural, legal, and technical protocols or practices that strengthen economies and societies."<sup>2</sup>

All OECD member countries should acknowledge and support in their policy, programmes 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.

## **1.1 Enabling ICT in Less Developed Regions**

OECD countries play a very significant role in many Less Developed Countries (LDC's) in the mode and pace of the development of the Information Economy and Society through Overseas Development Assistance (ODA), through their policy involvement through United Nations and other agencies in the regulatory and policy environment of LDC's, and through their influence on the manner and volume of Overseas Direct Investment including

---

<sup>2</sup> See Objectives of the Meeting, Organisation for Economic Co-operation and Development, The Future of the Internet Economy - OECD Ministerial Meeting - Seoul, Korea, June 17-18, 2008,

[http://www.oecd.org/document/19/0,2340,fr\\_2649\\_34255\\_38051667\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/19/0,2340,fr_2649_34255_38051667_1_1_1_1,00.html).

in LDC's. Among the issue areas where OECD countries may have influence with respect to Less Developed Countries are:

- The realization of widespread access to the Internet for economic and other purposes in many LDC's is dependent in part on the availability (and usability) of public Internet access facilities;
- The realization of equitable costs (and digital carriage volumes and quality) of regional and national interconnection to the global telecommunications and thus Internet access network remains a cause of concern for many countries particularly in sub-Saharan Africa;
- The Digital Divide as the division between those with Internet access and those without is often but a symptom of other "divides" limiting the "accessibility" of Internet based services such as 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;
- The challenge in Less Developed Countries is to extend to the widest possible range of users the opportunities that ICTs present that is they must also have access to the means to use the Internet in productive and meaningful ways;
- Civil Society also recognizes the exceptional difficulties (and opportunities) which Indigenous Peoples (IPs) experience in relation to having access to and making effective use of ICTs. Yet ICTs provide an instrument through which IPs 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 IPs to realize the opportunity for access and effective use of ICTs in support of their objectives;
- Civil Society believes that the Internet as a means for enabling the distribution of intelligence and empowerment to the edges of the network should be recognized and supported in the design and deployment of technical and related organizational and governance systems;
- There has been a dramatic decline in the cost of computing hardware in LDCs as elsewhere. This highlights the excessive cost of Internet access in many of these same countries resulting from managed pricing or lack of competition;
- Many of the services which in Developed Countries have been computer based, are, in LDC's cellular telephone based. 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. These developments should be encouraged and efforts should be made to integrate the variety of "more structured" development initiatives as cellular services in LDC's;
- Community Radio is 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.

All OECD member countries through their ODA programs, their policy involvement in the regulatory and policy environment of LDC's, and their

influence on the manner and volume of Overseas Direct Investment should support and promote:

- widespread access to the Internet through publicly supported public and community Internet Access points where appropriate;
- lower costs of interconnection for LDC's;
- active responses to ensure 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 ICTs 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 Peoples to realize the opportunity for access and effective use of ICTs in support of their objectives;
- promote deregulation and competitive development to reduce access costs and increase capacity in LDC's (as elsewhere);
- empowerment to the edges of the network through the design and deployment of appropriately designed technical and related organizational and governance systems;
- delivery of the range of services in support of the Information Economy and Society through cellular telephones in LDC's should be encouraged;
- support 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;

## **1.2 Non-Discrimination in Access**

Participation in economic life is becoming increasingly dependent on equitable access to the use of the Internet infrastructure. Barriers to such participation may be highly discriminatory in the determination of life chances and opportunities for personal well-being. Ensuring equitable and non-discriminatory access to this infrastructure is an essential component to be included in any e-economy policy framework. Among the barriers to equitable participation are:

- disability which interferes with the opportunity to make use of the input/output devices or places of (public) Internet access
- Illiteracy or significant low levels of literacy resulting from lower levels of education, cognitive abilities or limited facility with the language may impede digitally enabled activities which act as discriminants for those with 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;
- cost may result in differential access to the use of the Internet;

- gender has been linked with limited access or use of Internet opportunities including under-representation ICT decision-making capacities;
- those living in remote, rural, or low-income areas and particularly for Indigenous Peoples may experience additional difficulties (and costs) in obtaining access to the means for participation in the digital economy.
- individuals' relationship with specific access providers or their business partners may also be a source for discrimination against particular users. Vertical integration of access provision with other products, content, and services may lead access providers to engage in tying behaviors, such as blocking or degrading competitors' services. Competition and communications authorities should act to prevent such behavior.

All OECD member countries should implement:

- Standards for the design of web interfaces which enable utilization of these sites by those with visual and other disabilities which need to be enforced.
- Standards for determining the level of literacy required for utilization of specific sites and particularly public service sites need to be enforced.
- The widespread availability of publicly accessible Internet services (through community access points or telecenters) at no or nominal cost is a minimum basis for ensuring equitable participation in the Information Society.
- Training or support services in the context of the Public Internet Access sites needs to be provided to assist those who lack confidence or skill with respect to Internet use 5. 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 needs to be undertaken by Governments
- Actions to ensure that there is no discrimination or additional barriers to participation by residents of rural and remote regions thus public authorities may need to intervene to balance costs as between locales and regions.
- Vertical integration of access provision with other products, content, and services may lead access providers to engage in tying behaviors, such as blocking or degrading competitors' services. Competition and communications authorities should act to prevent such behavior.

## **2.0 Fuelling 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 Access to Knowledge (A2K) through new wealth generated in the transition to a global knowledge economy and the democratizing freedoms 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. It 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 globalised world. Intellectual Property (IP) law has 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.

In order to promote Access to Knowledge and preserve the public domain, 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 & limitations on copyright
- promote the procurement of open educational resources in public schools
- build infrastructure & capacity for Internet access in poor and rural areas

#### *Libraries*

- create robust exemptions for circumvention of DRM for libraries & research
- engage public-private partnerships enabling 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.

## 3. Ensuring Consumer and Privacy Protection and Building Confidence

### 3.1 Consumer Rights in the Digital Environment

Despite significant progress made by OECD countries over the past decade in addressing the obstacles to consumer confidence online, there remains much to be done if such confidence is to be maintained, let alone increased. Therefore we ask the OECD and its member governments to address, agree upon and define essential Consumer Rights in the Digital Environment, at the Future of the Internet Ministerial.

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) can expect public support, e.g. in the protection of anti-piracy technologies, only to the extent that DRMs respect the wider interests of public policy, public access, consumer rights, the promotion of competition and technological development. In particular, the potential anticompetitive effects of DRMs should be reviewed.

All OECD member countries should:

Ensure that consumer protection laws 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 criminalized;
- Right to choice, knowledge and cultural diversity;
- Right to defend and maintain consumer rights and fair commercial practices in the digital environment.

### 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<sup>3</sup>. 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<sup>4</sup>. The OECD Privacy Guidelines set out specific rules covering the collection, storage and dissemination of electronic data. They are as relevant in 2008 as they were in 1998, and provide a solid foundation for data

---

<sup>3</sup> See Universal Declaration of Human Rights, article 20(1) available at <http://www.un.org/Overview/rights.html>.

<sup>4</sup> Rotenberg, Marc. “Protecting Human Dignity in the Digital Age” (UNESCO 2000), available at [http://www.unesco.org/webworld/infoethics\\_2/eng/papers/paper\\_10.htm](http://www.unesco.org/webworld/infoethics_2/eng/papers/paper_10.htm).

protection in global networks. However, 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 governments are increasingly accessing databases for law enforcement, national security and other administrative purposes without provide the limitation and public accountability that traditionally have safeguard 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.

For these reasons, all OECD member countries should:

- adopt comprehensive data protection laws covering both public and private sector use of citizen data, and covering all private sector organizations;
- ensure such data protection laws should include effective enforcement mechanisms so as to ensure accountability and compliance;
- fund independent bodies with the mandate to protect privacy, and ensure that such bodies have sufficient resources to oversee privacy laws;
- 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, including through collection of data 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 mechanisms.

### **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. Such advertising is increasingly targeted and explicitly designed to influence consumers, including children, in highly subtle and covert ways. 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.

For these reasons, 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.

### **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.

For these reasons, 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).

### **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 it can provide great convenience, it can also pose certain risks that should be addressed now while still in the early stages of development.

For these reasons, 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.

### **3.3.4 Unsolicited Commercial Email: Spam**

Spam now accounts for the vast majority of email traffic on the Internet. In addition to being a nuisance, important messages lost in the flood of spam or captured by spam filtering tools, and costs ultimately paid by consumers for spam filtering by ISPs. 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.

For these reasons, all OECD member countries should:

- establish laws outlawing spam and procedures for holding spammers accountable, and should redouble their cooperative efforts to address cross-border aspects of the problem.

### **3.3.5 Cross-border dispute resolution**

The OECD and its member countries have done much work since 1998 on developing effective online dispute resolution (“ODR”) mechanisms so as to facilitate e-commerce. However, effective ODR options – i.e., mechanisms that are low cost, independent and fair – for consumers remain limited.

For these reasons, 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.

## **3.4 Identity Management**

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. 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 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.

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.

To Businesses and Developers:

- Companies who implement stronger authentication practices for online payment systems should not require consumers to accept more responsibility than reasonable;
- Businesses, who require consumers to use particular systems, should be held liable for losses incurred as a result of deficiencies of, or failures in their systems.

- Developers of authentication and ID management systems should ensure they are designed according to the principles of privacy and user-center.

### **3.5 Network Security and Prevention of Fraud**

Possibly the greatest impediment to consumer e-commerce is lack of security on the Internet. 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. At the same time there is a growing number of identity theft (ID theft) and other attacks, such as phishing, pharming and spoofing. 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.

For these reasons, 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.
- Enact or update national laws to deal with 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 and help-lines to help innocent victims of ID theft repair their financial affairs, including dedicated help-lines and international hot lines.

## **4.0 Benefiting from convergence**

### **4.1 Interoperability and open standards**

In order to achieve the interoperability necessary for the growth and convergence of the Internet and ICTs, hardware and software must use sets of common standards. Using open standards provides allows us to reap the full social and competitive benefits of convergence.

Open standards provide for this in a number of ways. They allow for competition by preventing technological lock-ins and other anti-competitive practices. Open standards also promote good governance principles, since in critical applications like voting machines, they allow for transparency. Open standards also promote civic involvement in democracy by ensuring that information flowing between the government and the public can be sent and

received by the entire public, and not just the consumers of one vendor's products. Open standards for documents and applications also aids in accessing archived materials, ensuring that digitization will not result in information becoming inaccessible due to technological obsolescence.

For these reasons, the 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.

## **4.2 Open broadband networks and net neutrality**

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 communications networks, discriminating service providers can lock consumers in to an anticompetitive environment that stifles technological growth and stymies 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.

For these reasons, 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.

The OECD should also:

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

For these reasons, 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.

### **4.3 Innovation and Copyright**

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.

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 the Internet and ICTs to make effective use of specific exceptions and limitations in national copyright law. 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. And 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.

For these reasons, OECD countries should:

- undertake research amongst OECD countries' laws 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 use in considering implementing legislative limitation of liability regimes, and entities within OECD countries that are developing policies and practices to implement such legal regimes.
- 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.