



Information Documents

SG/Inf(2008)14

17 September 2008

Internet - a critical resource for all

Document presented by the Secretary General of the Council of Europe to the Internet Governance Forum, Hyderabad, India, 3 - 6 December 2008

Executive Summary

An "Internet for all" is a legitimate aspiration linked to the prospects of development and democratic citizenship which must go hand in hand with a maximum of rights and services subject to a minimum of restrictions and a level of security which users are entitled to expect. Freedom of expression and information regardless of frontiers is an overarching requirement.

This involves access to the Internet service in its own right (including for people with disabilities, communities, people in a vulnerable situation or who are otherwise disadvantaged, and social groups including minority groups and the elderly) and also access to a range of services which make the lives of people, communities and groups more fulfilling. Only by ensuring access for all will the Internet realise its full public (service) value as an essential tool for everyday activities and its contribution to democracy.

Concrete examples of Council of Europe texts worked out in partnership with relevant stakeholders show how security, privacy and openness on the Internet are mutually reinforcing. They also exemplify our evolving response to the challenge of cybercrime, which has been broadly taken up across all continents. The Council's work in respect of child and health protection is ongoing.

The Council of Europe provides state and non-state actors with co-operation platforms, legal standards and public policy and practical tools which fit well the current transition towards a more definite rights and people-centred Internet governance approach. The legal and political frameworks being developed must take into account the needs (in access, security, privacy and openness terms) of both current (1.4 billion) and all future (including the next billion) Internet users.

Introduction

1. The overall IGF theme of an "Internet for all", together with the sub-themes "reaching the next billion", "promoting cybersecurity and trust" and "fostering security, privacy and openness", is based on the underlying belief that the Internet has the potential to improve our quality of life. It contributes to the United Nations Millennium Development Goals, and is linked to the prospects of economic and social development and the promotion of the values of the preservation of human society and civilisation, and the belief in individual freedom, political liberty and the rule of law which form the basis of all genuine democracies.

2. For the Council of Europe, as an international organisation which works to promote and protect democracy, human rights and the rule of law, an "Internet for all" is therefore a legitimate aspiration linked to the prospects of development and democratic citizenship which must go hand in hand with a maximum of rights and services subject to a minimum of restrictions and a level of security which users are entitled to expect.
3. The IGF is a unique community through which we can underscore and reinforce these values, rights and principles. It offers the ideal platform for dialogue and co-operation.

Reaching the next billion through greater accessibility and democracy

4. An "Internet for all" means accessibility for people with disabilities, communities, people in a vulnerable situation or who are otherwise disadvantaged, and social groups including minority groups and the elderly. This implies access to a range of services which make the lives of these people, communities and groups more fulfilling. Examples include secured electronic voting¹ and distance learning education programmes. We have to consider the Internet as both a service in its own right and as a means to reach other services. We must encourage the use of the Internet as a platform for dialogue, to encourage tolerance, mutual understanding and social cohesion. To this end, the creation and maintenance of public access points providing access for all to a minimum set of communication and information services and the provision of adequate facilities for the access to new communication and information services could be usefully discussed².
5. The Council of Europe recently stated that Internet services and tools for people with disabilities should be designed bearing in mind the need to

¹ Council of Europe Rec(2004)11 of the Committee of Ministers on legal, operational and technical standards for e-voting:
<http://wcd.coe.int/ViewDoc.jsp?id=778189&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75>

² Council of Europe Recommendation No. R (99) 14 of the Committee of Ministers on universal community service concerning new communication and information services:
[http://www.coe.int/t/dghl/standardsetting/media/Doc/CM/Rec\(1999\)014&ExpMem_en.asp#TopOfPage](http://www.coe.int/t/dghl/standardsetting/media/Doc/CM/Rec(1999)014&ExpMem_en.asp#TopOfPage)

achieve full participation through universal design. The promotion of equal rights for all citizens in all aspects of the information society should be underlined³ as should the equal delivery of Internet tools and services which are compatible with other assistive technological devices⁴.

6. One of the Council of Europe's main objectives is to reach full participation of all citizens and other stakeholders, in particular through the transparency of governments and in accessing information. Stakeholders cannot form and voice their opinions well if they do not have access to information. Governments at all levels should therefore focus on providing information through the Internet as part of the public value and general openness of the Internet⁵.
7. In this connection, there is a trilateral initiative underway between the Council of Europe, the United Nations Economic Commission for Europe (UNECE) and the Association for Progressive Communications (APC) to prepare a code of good practice on public participation, access to information and transparency in Internet governance. This code will enable all institutions playing a role in governing the Internet to commit themselves to ensuring transparency, public participation of all stakeholders and access to information in Internet governance.
8. Citizens and other stakeholders should have more options and possibilities to be involved in democracy online (e.g. via games consoles with online features). It would be useful for the IGF to discuss the transparency, accountability and responsiveness of democratic institutions and the potential benefits for democratic societies (e.g. inclusiveness, accessibility and participation, social cohesion) with regard to the Internet and its openness. Council of Europe principles and guidelines on these and other aspects of e-democracy will be finalised in the coming months.

³ Council of Europe Resolution ResAP(2007)3 of the Committee of Ministers on "Achieving full participation through Universal Design": <https://wcd.coe.int/ViewDoc.jsp?id=1226267&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75>

⁴ Council of Europe Resolution ResAP(2001)3 "Towards full citizenship of persons with disabilities through inclusive new technologies": <http://wcd.coe.int/ViewDoc.jsp?id=233261&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75>

⁵ Council of Europe Forum for the Future of Democracy & Project "Good Governance in the Information Society": <http://www.coe.int/T/E/Integrated%5FProjects/Democracy>

9. An important prerequisite for achieving an "Internet for all" is open design. Governments and other stakeholders should be encouraged to use open standards and open source software to communicate, in particular as a means of promoting independence (of suppliers), freedom of choice, interoperability, digital durability, transparency and accountability.

Fostering security, privacy and openness

10. Security, privacy and openness on the Internet are mutually reinforcing pre-conditions for users, including the next billion users, to be able to freely express themselves and to access information. By stepping up levels of user security and privacy their confidence to use the Internet will grow.
11. On this basis, the Internet is becoming an essential tool for everyday activities (communication, information, knowledge, commercial transactions, entertainment). There will be a greater demand for Internet services and, as a corollary, there will be a greater legitimate expectation that such services will be *inter alia* secure and reliable.
12. IGF discussions on the security, privacy and openness of the Internet should include reflections on the public value of the Internet bearing in the mind the Council of Europe's guidelines on the public service value of the Internet⁶ which explicitly address and map out measures to promote openness, security and privacy on the Internet. These measures, agreed by the 47 member States of the Council, include the following:

...as regards security and privacy:

"- (...) implement a common criminal policy aimed at the protection of society against cybercrime, to co-operate for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence, and to resolve jurisdictional problems in cases of crimes committed in other states parties to the Cybercrime convention;

(...)

⁶ Council of Europe Recommendation CM/Rec(2007)16 of the Committee of Ministers on measures to promote the public service value of the Internet:
<http://wcd.coe.int/ViewDoc.jsp?id=1207291&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75>

- enhance network and information security to enable them to resist actions that compromise their stability as well as the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems;

- empower stakeholders to protect network and information security;

- adopt legislation and establishing appropriate enforcement authorities, where necessary, to combat spam. Member states should also facilitate the development of appropriate technical solutions related to combating spam, improve education and awareness among all stakeholders and encourage industry-driven initiatives, as well as engage in cross-border spam enforcement co-operation;

- encourage the development of common rules on the co-operation between providers of information society services and law enforcement authorities ensuring that such co-operation has a clear legal basis and respects privacy regulations;

- protect personal data and privacy on the Internet and other ICTs (to protect users against the unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorised disclosure of such data, or against the intrusion of their privacy through, for example, unsolicited communications for direct marketing purposes) and harmonising legal frameworks in this area without unjustifiably disrupting the free flow of information, in particular by:

a. improving their domestic frameworks for privacy law in accordance with Article 8 of the European Convention on Human Rights and by signing and ratifying the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108);

b. providing appropriate safeguards for the transfer of international personal data to states which do not have an adequate level of data protection;

c. facilitating cross-border co-operation in privacy law enforcement;

- combat piracy in the field of copyright and neighbouring rights;

- work together with the business sector and consumer representatives to ensure e-commerce users are afforded transparent and effective consumer protection that is not less than the level of protection afforded in other forms of commerce. This may include the introduction of requirements concerning contracts which can be concluded by electronic means, in particular requirements concerning secure electronic signatures;

- promote the safer use of the Internet and of ICTs, particularly for children, fighting against illegal content and tackling harmful and, where necessary, unwanted content through regulation, the encouragement of self-regulation, including the elaboration of codes of conduct, and the development of adequate technical standards and systems;

- promote the signature and ratification of the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201). "

...as regards openness:

"- promote the active participation of the public in using, and contributing content to, the Internet and other ICTs;

- promote freedom of communication and creation on the Internet, regardless of frontiers, in particular by:

a. not subjecting individuals to any licensing or other requirements having a similar effect, nor any general blocking or filtering measures by public authorities, or restrictions that go further than those applied to other means of content delivery;

b. facilitating, where appropriate, "re-users", meaning those wishing to exploit existing digital content resources in order to create future content or services in a way that is compatible with respect for intellectual property rights;

c. promoting an open offer of services and accessible, usable and exploitable content via the Internet which caters to the different needs of users and social groups, in particular by:

- allow service providers to operate in a regulatory framework which guarantees them non-discriminatory access to national and international telecommunication networks;

- increase the provision and transparency of their online services to citizens and businesses;

- engage with the public, where appropriate, through user-generated communities rather than official websites;

- encourage, where appropriate, the re-use of public data by non-commercial users, so as to allow every individual access to public information, facilitating their participation in public life and democratic processes;

- promote public domain information accessibility via the Internet which includes government documents, allowing all persons to participate in the process of government; information about personal data retained by public entities; scientific and historical data; information on the state of technology, allowing the public to consider how the information society might guard against information warfare and other threats to human rights; creative works that are part of a shared cultural base, allowing persons to participate actively in their community and cultural history;[...]"

13. The above-mentioned principles and guidelines provide a blueprint for IGF discussions on the engagements and commitments of states, in co-operation with the private sector and civil society, for openness, security and privacy within a human rights framework.

Human rights guidelines for Internet service providers

14. Accessing the Internet via, and using the tools and services offered by, Internet service providers (ISPs) are integral elements of an "Internet for all". The potential for ISPs to foster freedom of communication on the Internet merits discussion in the IGF, in particular because they can help to foster users' privacy and security. The Council of Europe's guidelines and principles on the legitimate, proportional and transparent use of Internet filters provide a good starting point for such discussion⁷.

⁷ Council of Europe Recommendation CM/Rec(2008)6 of the Committee of Ministers on measures to promote the respect for freedom of expression and information with regard to Internet filters:

[http://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec\(2008\)6&Language=lanEnglish&Ver=original&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75](http://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec(2008)6&Language=lanEnglish&Ver=original&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75)

15. Moreover, in co-operation with the European Internet Service Providers Association (EuroISPA), the Council of Europe has prepared new human rights guidelines for ISPs which foster Internet access and users' security and privacy on the Internet. In particular, the guidelines encourage ISPs *inter alia*:

- a. to foster users' general openness towards the Internet (i.e. their ability to express and inform themselves) by explaining how to deal with illegal and harmful content, how to complain/obtain redress (e.g. right of reply), and how to use specific application services (e.g. chat rooms, discussion forums) and tools offered by them (e.g. spam filters);
- b. to foster the openness of ISP services *inter alia* by encouraging their reflections on users' rights and freedoms when blocking or degrading the quality of their services, cutting Internet access, installing filters with regard to their legitimacy, proportionality and transparent use, and when following procedures to monitor, intercept and delete users correspondence;
- c. to protect users against security risks (e.g. such as viruses, worms, trojans, 'phishing') and privacy risks (e.g. spyware, profiling, disclosure of identification, connection and traffic data to law enforcement) by informing and guiding them with information and advice;
- d. not to reveal the identity of users (unless there is a legal duty to do so), their traffic data or the content accessed by them to third parties, and to establish appropriate procedures to protect such traffic and content data, especially by ensuring data integrity, confidentiality as well as physical and logical security of the network and services provided;
- e. not to generally collect, process or store data about users (unless for legitimate purposes in accordance with data protection laws) nor to use this data for commercial purposes.

Human rights guidelines for online games providers

16. The openness of the Internet includes the reliance on it to provide everyday activities such as entertainment and, as a corollary, the (economic) freedom to offer online entertainment services.

17. In co-operation with the Interactive Software Federation of Europe (ISFE), the Council of Europe has prepared new human rights guidelines for the developers and publishers of online games which raise awareness of the risk of harm, especially for children, concerning content in gaming (e.g. gratuitous portrayal of violence, inhuman, cruel, sexist and degrading content, open and concealed messages of aggressive nationalism, ethnocentrism, xenophobia, racism and intolerance) and the security and privacy risks for gamers who play and communicate with each other through games. Whilst encouraging expression and openness in and through online gaming communities, the Council's guidelines underline the need for openness and transparency about the security and privacy risks of gaming.

Protecting children's dignity, security and privacy on the Internet

18. The Internet is an unparalleled tool and platform for children and young people to communicate, express and inform themselves in the exercise of their right to freedom of expression to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers (Article 10 of the European Convention on Human Rights). It should be underlined that children's well-being in online environments is not only about their risks and need for protection (e.g. against sexual exploitation and abuse committed via the Internet) but is also about their positive online experiences, in participating and having the skills to participate actively and positively. After all, the European Convention on Human Rights applies to adults as much as it applies to children.
19. The openness, security and privacy of the Internet with regard to the well-being of children is of fundamental importance for the Internet's future in reaching the next billion users. IGF discussions should bear in mind the 1989 United Nations Convention of the Rights of the Child which underlines the inherent right for children to dignity, to special protection and care for their well-being, to protection against all forms of discrimination or arbitrary or unlawful interference with their privacy and to unlawful attacks on their honour and reputation.
20. In this connection, the Council of Europe has been leading discussions on ways to deal with the 'electronic footprint' of children as a means to encourage their freedom, confidence and trust in using the Internet. By learning how to make the Internet forget about 'child generated content', children's security can be improved (i.e. by removing traces of their personal details). The profiling of information and the retention of

personal data concerning children's activities for commercial purposes and the misuse of information gathered about children's online traces (e.g. educational bodies and prospective employers reaching decisions about young adults from information gathered via the Internet) is a cause of concern that should be addressed in IGF discussions.

21. Overall, Council of Europe member States have declared that, other than in the context of law enforcement, there should be no lasting or permanently accessible record of the content created by children on the Internet which challenges their dignity, security and privacy or otherwise renders them vulnerable now or at a later stage in their lives. It is incumbent on the Council and its member states to explore the feasibility of removing or deleting such content, including its traces (logs, records and processing), within a reasonably short period of time⁸.

Meeting the challenge of cybercrime

22. From a human rights perspective, taking into account its arsenal of globally reaching international instruments (in particular as regards cybercrime, prevention of terrorism, data protection, action against trafficking in human beings, and the protection against sexual exploitation and abuse of children), the Council of Europe is providing tools, co-operation platforms and inspiration for states and other stakeholders to foster security and privacy on the Internet.
23. The Cybercrime Convention⁹ and the international co-operation and assistance facilitated by the Council provide both a legal response and a platform from which states and other stakeholders can make legal, political and practical progress to meet the challenge of cybercrime. The Council of Europe does this in particular by:

⁸ Council of Europe Declaration of the Committee of Ministers on protecting the dignity, security and privacy of children on the Internet:
[http://wcd.coe.int/ViewDoc.jsp?Ref=Decl\(20.02.2008\)&Language=lanEnglish&Ver=0001&Site=COE&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75](http://wcd.coe.int/ViewDoc.jsp?Ref=Decl(20.02.2008)&Language=lanEnglish&Ver=0001&Site=COE&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75)

⁹ www.coe.int/cybercrime for the Convention on Cybercrime (CETS 185) and Council of Europe theme file on Cybercrime: a threat to democracy, human rights and the rule of law:
http://www.coe.int/t/dc/files/themes/cybercrime/default_en.asp

- encouraging states across the world to use the Convention on Cybercrime Convention as a “model law” when developing national legislation;
 - providing technical assistance and expertise to states when elaborating legislation and preparing to sign, ratify or accede to the Cybercrime Convention;
 - assisting national authorities in the implementation of the Cybercrime Convention via the Project on Cybercrime;
 - encouraging states to fully co-operate internationally against cybercrime, in particular through the network of national 24/7 points of contact¹⁰ and the framework provided by the Convention on Cybercrime;
 - helping law enforcement authorities and Internet service providers to work together by using the Council’s guidelines on co-operation as a means to structure and organise their co-operation when investigating cybercrime.¹¹
24. The Council of Europe is co-operating with a wide range of public and private sector partners and international organisations to create synergies, promote convergence and provide best possible support and guidance to states worldwide.
25. By mid-2008, more than 100 countries from all continents have been using the Convention on Cybercrime as a guideline or reference when developing new legislation or reviewing and improving existing laws related to cybercrime. In addition to member States of the Council of Europe several other countries have signed (Canada, Japan, South Africa) or ratified (United States of America) this treaty or have been invited to accede (Costa Rica, Mexico, Philippines), and the accession by other countries is under consideration. There is thus a global trend towards the strengthening of cybercrime legislation in a harmonised manner on the basis of this Convention.

¹⁰ Council of Europe website on 24/7 points of contact:
http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/Points%20of%20Contact/aboutPoC_en.asp

¹¹ Council of Europe guidelines for the cooperation between law enforcement authorities and ISPs (April 2008):
http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/cy_activity_Interface2008/567_prov-d-guidelines_provisional2_3April2008_en.pdf

26. Therefore, any suggestion to develop new "model legislation" or another treaty on cybercrime is not helpful. This creates uncertainty, diverts attention and resources, and in particular carries the risk of divergence. It is essential that all partners engage in a co-operative effort and provide clear guidance to countries worldwide by making use of existing instruments.

Countering the terrorist use of the Internet¹²

27. Using the Internet for non-democratic purposes (e.g. online terrorist acts, cybercrime etc) could also be addressed. The IGF could discuss the potential risks and damage to democracy and openness when such acts occur as well as the most effective ways of countering such threats.

28. In alleviating the security risks associated with the terrorist use of the Internet, IGF discussions could usefully focus on states' implementation of and accession to the following international treaties:

- a. the Cybercrime Convention, in particular as regards (i) Articles 4 and 5 on data and system interference which include denial of service attacks, (ii) procedural provisions to facilitate investigations related to computer systems, (iii) Chapter 3 providing for efficient international co-operation;
- b. the Convention on the Prevention on Terrorism¹³, in particular as regards criminalising the public provocation of acts of terrorism, training and recruitment, and facilitating international co-operation.

Consumer protection from counterfeit medicines and medical devices

29. There is an urgent need for health protection from counterfeit or illegal medical products (medicines and medical devices) offered and sold via the

¹² Council of Europe theme file on Terrorism: the worst enemy of democracy:
http://www.coe.int/t/dc/files/themes/terrorisme/default_en.asp

¹³ Council of Europe Convention on the Prevention of Terrorism
CETS No.: 196:
<http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=196&CM=8&DF=8/24/2007&CL=ENG>

- internet. The perceived advantages of these products online (e.g. easier access, lower prices, purchaser discretion) underlines the need for consumers to make informed choices bearing in mind the health risks and the exposure of their personal data, identity and anonymity.
30. There should be effective strategies which encompass a set of concerted measures, including public awareness-raising about how to avoid risky offers and discern dubious information on the web, and a regulatory, commercial, social and health environment which makes convenience safer without detrimental consequences for health, private and public financial means.
 31. Council of Europe work is effectively combating these risks and developing strategies in various ways, most notably in:
 - a. preparing an international legal instrument on the counterfeiting of medical products and similar crimes involving threats to public health;
 - b. setting standards on good practices for distributing medicines via mail order which facilitates the protection of patient safety and the quality of delivered medicine¹⁴;
 - c. implementing special work programmes to protect public health from counterfeit medicines and similar crimes (e.g. risk management and prevention strategies, model approaches for multi-disciplinary co-operation, knowledge building, regular training).

An Internet for all made effective by better co-operation between stakeholders

32. An "Internet for all" is dependent on it being trustworthy and reliable to use. This can only be achieved if there is constructive co-operation between stakeholders. It is counter-productive for actors to work in isolation from each other. Calls for a global convention on Internet

¹⁴ Council of Europe Resolution ResAP(2007)2 of the Committee of Ministers on good practices for distributing medicines via mail order which protect patient safety and the quality of the delivered medicine:
[http://wcd.coe.int/ViewDoc.jsp?Ref=ResAP\(2007\)2&Language=lanEnglish&Ver=original&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75](http://wcd.coe.int/ViewDoc.jsp?Ref=ResAP(2007)2&Language=lanEnglish&Ver=original&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75)

freedom and the limitations of corporate social responsibility serve to underline the importance of such co-operation.

33. IGF discussion on the roles and responsibilities of state and non-state actors within a clear legal framework and using complementary regulatory frameworks is necessary as a means of *inter alia* improving protection and respect for human rights in online environments.
34. The European Dialogue on Internet Governance (EuroDIG)¹⁵, to be hosted by the Council of Europe in October 2008, will highlight European issues and concerns regarding *inter alia* the interplay between security, privacy, and openness as concepts that can be fostered simultaneously and can even mutually reinforce each other.
35. The IGF process is helping the Council of Europe to break new ground about the way in which governments communicate with other stakeholders, in particular the private sector and civil society, and is increasingly enabling us to foster multi-stakeholder dialogue in intergovernmental settings.

Conclusions

36. The IGF should take into consideration that the Council of Europe is providing state and non-state actors with a range of almost ready-made tools, co-operation platforms, legal standards and public policy measures to advance the legal and political frameworks dealing with the fight against cybercrime, cybersecurity and trust, online political participation and the security and privacy risks on the Internet. In this connection, the public value of the Internet should be examined *inter alia* to ensure that the Internet remains an open and accessible space for all.

¹⁵ EuroDIG will take place in Strasbourg on 20 and 21 October 2008 : www.eurodig.org