United Nations A/HRC/17/27

General Assembly

Distr.: General
16 May 2011

Original: English

Human Rights Council
Seventeenth session
Agenda item 3
Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development

Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*

Summary

This report explores key trends and challenges to the right of all individuals to seek, receive and impart information and ideas of all kinds through the Internet. The Special Rapporteur underscores the unique and transformative nature of the Internet not only to enable individuals to exercise their right to freedom of opinion and expression, but also a range of other human rights, and to promote the progress of society as a whole. Chapter III of the report underlines the applicability of international human rights norms and standards on the right to freedom of opinion and expression to the Internet as a communication medium, and sets out the exceptional circumstances under which the dissemination of certain types of information may be restricted. Chapters IV and V address two dimensions of Internet access respectively: (a) access to content; and (b) access to the physical and technical infrastructure required to access the Internet in the first place. More specifically, chapter IV outlines some of the ways in which States are increasingly censoring information online, namely through: arbitrary blocking or filtering of content; criminalization of legitimate expression; imposition of intermediary liability; disconnecting users from Internet access, including on the basis of intellectual property rights law; cyber-attacks; and inadequate protection of the right to privacy and data protection. Chapter V addresses the issue of universal access to the Internet. The Special Rapporteur intends to explore this topic further in his future report to the General Assembly. Chapter VI contains the Special Rapporteur's conclusions and recommendations concerning the main subjects of the report.

* Late submission.

The first addendum to the report comprises a summary of communications sent by the Special Rapporteur between 20 March 2010 and 31 March 2011, and the replies received from Governments. The second and third addenda contain the findings of the Special Rapporteur's missions to the Republic of Korea and Mexico respectively.

Contents

I. Introduction

1. The present report is submitted to the Human Rights Council by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression pursuant to Human Rights Council resolution 7/36. In particular, the resolution requests the Special Rapporteur "to continue to provide his/her views, when appropriate, on the advantages and challenges of new information and communication technologies, including the Internet and mobile technologies, for the exercise of the right to freedom of opinion and expression, including the right to seek, receive and impart information and the relevance of a wide diversity of sources, as well as access to the information society for all".[1] On this basis, the report expands upon the previous mandate holders' reports on topics related to the Internet,[2] taking into account recent developments and information gathered through five regional consultations organized by the Special Rapporteur in 2010 and 2011.[3]

2. While the Internet has been in existence since the 1960s, its current use throughout the world across different age groups, and incorporation into virtually every aspect of modern human life, has been unprecedented. According to the International Telecommunication Union, the total number of Internet users worldwide is now over 2 billion.[4] Active users of Facebook, an online social networking platform, grew from 150 million to 600 million between 2009 and 2011. The Special Rapporteur believes that the Internet is one of the most powerful instruments of the 21st century for increasing transparency in the conduct of the powerful, access to information, and for facilitating active citizen participation in building democratic societies. Indeed, the recent wave of demonstrations in countries across the Middle East and North African region has shown the key role that the Internet can play in mobilizing the population to call for justice, equality, accountability and better respect for human rights. As such, facilitating access to the Internet for all individuals, with as little restriction to online content as possible, should be a priority for all States.

3. In this regard, the Special Rapporteur would like to underscore that access to the Internet has two dimensions: access to online content, without any restrictions except in a few limited cases permitted under international human rights law; and the availability of the necessary infrastructure and information communication technologies, such as cables, modems, computers and software, to access the Internet in the first place. The first dimension is addressed in Chapter IV of the report, which outlines some of the ways in which States are restricting the flow of information online through increasingly sophisticated means. The second dimension is examined in Chapter IV. The Special Rapporteur intends to explore the latter issue further in his future report to the General Assembly.

[1] Human Rights Council resolution 7/36, para. 4(f).

[2] E/CN.4/1998/40; E/CN.4/1999/64; E/CN.4/2000/63; E/CN.4/2001/64; E/CN.4/2002/75; E/CN.4/2005/64; E/CN.4/2006/55; A/HRC/4/27; A/HRC/7/14.

[3] See para. 5 for further information.

[4] International Telecommunication Union, StatShot No.5, January 2011 Available from: http://www.itu.int/net/pressoffice/stats/2011/01/index.aspx.

II. Activities of the Special Rapporteur

A. Communications

4. Between 20 March 2010 and 31 March 2011, the Special Rapporteur sent 195 communications, 188 of which were submitted jointly with other special procedures mandate holders. The geographical distribution of the communications was as follows: 29 per cent for Asia and the Pacific; 26 per cent for the Middle East and North Africa; 16 per cent for Africa; 15 per cent for Latin America and the Caribbean; and 14 per cent for Europe, Central Asia and North America. The summary of communications sent and replies received from Governments can be found in the first addendum to this report (A/HRC/17/27/Add.1).

B. Participation in meetings and seminars

5. The Special Rapporteur, with the support of local organizations, organized a series of expert regional consultations, beginning in March 2010 in Stockholm, followed by Buenos Aires (18-19 October 2010), Bangkok (18-19 November 2010), Cairo (11-13 January 2011), Johannesburg (15-16 February 2011), and Delhi (2-3 March 2011). The regional consultations concluded on 30 March 2011 with an expert meeting in Stockholm, organized by the Ministry of Foreign Affairs of Sweden. These meetings brought together experts and human rights defenders working on a range of Internet and freedom of expression-related issues in order to better understand their experience, needs and priorities in different countries and regions for the purposes of this report.

6. From 14 to 17 September 2010, the Special Rapporteur attended the Fifth Internet Governance Forum in Vilnius.

7. On 30 November 2010, the Special Rapporteur participated in an expert round table entitled “Equality, Non-discrimination and Diversity: Challenge or Opportunity for the Mass Media?” in Geneva, organized by the Office of the High Commissioner for Human Rights (OHCHR).

8. On 9 and 10 February 2011 and on 6 and 7 April 2011, the Special Rapporteur participated as an expert in the regional expert workshops on the prohibition of incitement to national, racial or religious hatred organized by OHCHR in Vienna and Nairobi respectively.

9. On 16 March 2011, the Special Rapporteur shared his views regarding the compatibility of blocking child pornography on the Internet with the right to freedom of expression in the context of discussions on the proposal for a directive of the European Parliament and of the Council on combating the sexual abuse and sexual exploitation of children and child pornography.

10. The Special Rapporteur also participated in a series of academic events in other countries, including Guatemala, Mexico, the Philippines, South Africa, Sweden and the United States of America.

C. Country visits

11. The Special Rapporteur notes that country visits remain central to his mandate. Requests sent to Governments to undertake a country mission are based on several factors, such as visits undertaken and requested by the former mandate holders, trends that emerge from communications sent on alleged violations of the right to freedom of opinion and

expression, and consideration of geographical balance. The Special Rapporteur hopes that visit requests will be favourably received by the Governments concerned.

1. Missions undertaken in 2010 and 2011

12. From 5 to 15 May 2010, the Special Rapporteur undertook a mission to the Republic of Korea. The mission report is included as an addendum to this report (A/HRC/17/27/Add.2).

13. From 10 to 21 August 2010, the Special Rapporteur undertook a mission to Mexico, together with the Special Rapporteur for Freedom of Expression for the Inter-American Commission on Human Rights, Catalina Botero. The mission report is included as an addendum to this report (A/HRC/17/27/Add.3).

14. From 3 to 5 April 2011, the Special Rapporteur visited the Republic of Hungary, at the invitation of the Government, to provide expert advice to the Government regarding Hungarian media legislation. The press release with his conclusions and recommendations can be found on the OHCHR website.[5]

15. From 10 to 17 April 2011, the Special Rapporteur undertook a mission to Algeria. The mission report will be presented at a future session of the Human Rights Council in 2012. The press release with his initial conclusions and recommendations can be found on the OHCHR website.[6]

2. Upcoming missions

16. The visit to Israel and the occupied Palestinian territory, which was scheduled to take place in May 2011, has been postponed. The new dates of the visit have yet to be agreed upon.

17. The Special Rapporteur would like to thank the Italian Government for its letter dated 6 August 2010 in response to his request for a visit. He hopes that a mutually convenient set of dates can be agreed upon for a visit in 2011.

3. Pending requests

18. As of March 2011, the following visit requests from the Special Rapporteur were pending: the Islamic Republic of Iran (requested in February 2010), Sri Lanka (requested in June 2009), Tunisia (requested in 2009), and the Bolivarian Republic of Venezuela (requested in 2003 and 2009).

III. General principles on the right to freedom of opinion and expression and the Internet

19. Very few if any developments in information technologies have had such a revolutionary effect as the creation of the Internet. Unlike any other medium of communication, such as radio, television and printed publications based on one-way transmission of information, the Internet represents a significant leap forward as an interactive medium. Indeed, with the advent of Web 2.0 services, or intermediary platforms that facilitate participatory information sharing and collaboration in the creation of content, individuals are no longer passive recipients, but also active publishers of information. Such

[5] Available from: http://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=10916&LangID=E.

[6] Ibid.

platforms are particularly valuable in countries where there is no independent media, as they enable individuals to share critical views and to find objective information. Furthermore, producers of traditional media can also use the Internet to greatly expand their audiences at nominal cost. More generally, by enabling individuals to exchange information and ideas instantaneously and inexpensively across national borders, the Internet allows access to information and knowledge that was previously unattainable. This, in turn, contributes to the discovery of the truth and progress of society as a whole.

20. Indeed, the Internet has become a key means by which individuals can exercise their right to freedom of opinion and expression, as guaranteed by article 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. The latter provides that:

(a) Everyone shall have the right to hold opinions without interference;

(b) Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice;

(c) The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:

(d) for respect of the rights or reputations of others;

(e) for the protection of national security or of public order (*ordre public*), or of public health or morals.

21. By explicitly providing that everyone has the right to express him or herself through any media, the Special Rapporteur underscores that article 19 of the Universal Declaration of Human Rights and the Covenant was drafted with foresight to include and to accommodate future technological developments through which individuals can exercise their right to freedom of expression. Hence, the framework of international human rights law remains relevant today and equally applicable to new communication technologies such as the Internet.

22. The right to freedom of opinion and expression is as much a fundamental right on its own accord as it is an “enabler” of other rights, including economic, social and cultural rights, such as the right to education and the right to take part in cultural life and to enjoy the benefits of scientific progress and its applications, as well as civil and political rights, such as the rights to freedom of association and assembly. Thus, by acting as a catalyst for individuals to exercise their right to freedom of opinion and expression, the Internet also facilitates the realization of a range of other human rights.

23. The vast potential and benefits of the Internet are rooted in its unique characteristics, such as its speed, worldwide reach and relative anonymity. At the same time, these distinctive features of the Internet that enable individuals to disseminate information in “real time” and to mobilize people has also created fear amongst Governments and the powerful. This has led to increased restrictions on the Internet through the use of increasingly sophisticated technologies to block content, monitor and identify activists and critics, criminalization of legitimate expression, and adoption of restrictive legislation to justify such measures. In this regard, the Special Rapporteur also emphasizes that the existing international human rights standards, in particular article 19, paragraph 3, of the International Covenant on Civil and Political Rights, remain pertinent in determining the types of restrictions that are in breach of States’ obligations to guarantee the right to freedom of expression.

24. As set out in article 19, paragraph 3, of the Covenant, there are certain exceptional types of expression which may be legitimately restricted under international human rights law, essentially to safeguard the rights of others. This issue has been examined in the previous annual report of the Special Rapporteur.[7] However, the Special Rapporteur deems it appropriate to reiterate that any limitation to the right to freedom of expression must pass the following three-part, cumulative test:

(a) It must be provided by law, which is clear and accessible to everyone (principles of predictability and transparency); and

(b) It must pursue one of the purposes set out in article 19, paragraph 3, of the Covenant, namely (i) to protect the rights or reputations of others, or (ii) to protect national security or of public order, or of public health or morals (principle of legitimacy); and

(c) It must be proven as necessary and the least restrictive means required to achieve the purported aim (principles of necessity and proportionality).

Moreover, any legislation restricting the right to freedom of expression must be applied by a body which is independent of any political, commercial, or other unwarranted influences in a manner that is neither arbitrary nor discriminatory, and with adequate safeguards against abuse, including the possibility of challenge and remedy against its abusive application.

25. As such, legitimate types of information which may be restricted include child pornography (to protect the rights of children),[8] hate speech (to protect the rights of affected communities),[9] defamation (to protect the rights and reputation of others against unwarranted attacks), direct and public incitement to commit genocide (to protect the rights of others),[10] and advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence (to protect the rights of others, such as the right to life).[11]

26. However, in many instances, States restrict, control, manipulate and censor content disseminated via the Internet without any legal basis, or on the basis of broad and ambiguous laws, without justifying the purpose of such actions; and/or in a manner that is clearly unnecessary and/or disproportionate to achieving the intended aim, as explored in the following sections. Such actions are clearly incompatible with States' obligations under international human rights law, and often create a broader "chilling effect" on the right to freedom of opinion and expression.

27. In addition, the Special Rapporteur emphasizes that due to the unique characteristics of the Internet, regulations or restrictions which may be deemed legitimate and proportionate for traditional media are often not so with regard to the Internet. For example, in cases of defamation of individuals' reputation, given the ability of the individual concerned to exercise his/her right of reply instantly to restore the harm caused, the types of sanctions that are applied to offline defamation may be unnecessary or disproportionate.

[7] A/HRC/14/23, paras. 72 - 87.

[8] Dissemination of child pornography is prohibited under international human rights law, see e.g. Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, art. 3, para. 1(c).

[9] See for example *Faurisson v. France*, United Nations Human Rights Committee, communication 550/1993, views of 8 November 1996. The issue of hate speech has also been addressed in previous reports, see inter alia E/CN.4/1999/64; E/CN.4/2000/63; E/CN.4/2002/75; and A/HRC/4/27.

[10] See for example article 3(c) of the Convention on the Prevention and Punishment of the Crime of Genocide.

[11] See for example article 20, paragraph 2, of the International Covenant on Civil and Political Rights.

Similarly, while the protection of children from inappropriate content may constitute a legitimate aim, the availability of software filters that parents and school authorities can use to control access to certain content renders action by the Government such as blocking less necessary, and difficult to justify.[12] Furthermore, unlike the broadcasting sector, for which registration or licensing has been necessary to allow States to distribute limited frequencies, such requirements cannot be justified in the case of the Internet, as it can accommodate an unlimited number of points of entry and an essentially unlimited number of users.[13]

IV. Restriction of content on the Internet

28. As outlined under Chapter III, any restriction to the right to freedom of expression must meet the strict criteria under international human rights law. A restriction on the right of individuals to express themselves through the Internet can take various forms, from technical measures to prevent access to certain content, such as blocking and filtering, to inadequate guarantees of the right to privacy and protection of personal data, which inhibit the dissemination of opinions and information. The Special Rapporteur is of the view that the arbitrary use of criminal law to sanction legitimate expression constitutes one of the gravest forms of restriction to the right, as it not only creates a "chilling effect", but also leads to other human rights violations, such as arbitrary detention and torture and other forms of cruel, inhuman or degrading treatment or punishment.

A. Arbitrary blocking or filtering of content

29. Blocking refers to measures taken to prevent certain content from reaching an end-user. This includes preventing users from accessing specific websites, Internet Protocol (IP) addresses, domain name extensions, the taking down of websites from the web server where they are hosted, or using filtering technologies to exclude pages containing keywords or other specific content from appearing. For example, several countries continue to block access to YouTube,[14] a video-sharing website on which users can upload, share and view videos. China, which has in place one of the most sophisticated and extensive systems for controlling information on the Internet, has adopted extensive filtering systems that block access to websites containing key terms such as "democracy" and "human rights".[15] The Special Rapporteur is deeply concerned that mechanisms used to regulate and censor information on the Internet are increasingly sophisticated, with multi-layered controls that are often hidden from the public.

30. The Special Rapporteur is also concerned by the emerging trend of timed (or "just-in-time") blocking to prevent users from accessing or disseminating information at key political moments, such as elections, times of social unrest, or anniversaries of politically or historically significant events. During such times, websites of opposition parties, independent media, and social networking platforms such as Twitter and Facebook are

[12] Center for Democracy & Technology, "Regardless of Frontiers: The International Right to Freedom of Expression in the Digital Age," version 0.5 - Discussion draft (April 2011), p.5.

[13] However, this does not apply to registration with a domain name authority for purely technical reasons or rules of general application which apply without distinction to any kind of commercial operation.

[14] See OpenNet Initiative, "YouTube Censored: A Recent History". Available from: http://opennet.net/youtube-censored-a-recent-history.

[15] Reporters without Borders, "Enemies of the Internet," March 2010. Available from: http://en.rsf.org/IMG/pdf/Internet_enemies.pdf, pp. 8-12.

blocked, as witnessed in the context of recent protests across the Middle East and North African region. In Egypt, users were disconnected entirely from Internet access.

31. States' use of blocking or filtering technologies is frequently in violation of their obligation to guarantee the right to freedom of expression, as the criteria mentioned under chapter III are not met. Firstly, the specific conditions that justify blocking are not established in law, or are provided by law but in an overly broad and vague manner, which risks content being blocked arbitrarily and excessively. Secondly, blocking is not justified to pursue aims which are listed under article 19, paragraph 3, of the International Covenant on Civil and Political Rights, and blocking lists are generally kept secret, which makes it difficult to assess whether access to content is being restricted for a legitimate purpose. Thirdly, even where justification is provided, blocking measures constitute an unnecessary or disproportionate means to achieve the purported aim, as they are often not sufficiently targeted and render a wide range of content inaccessible beyond that which has been deemed illegal. Lastly, content is frequently blocked without the intervention of or possibility for review by a judicial or independent body.

32. The Special Rapporteur notes that child pornography is one clear exception where blocking measures can be justified, provided that the national law is sufficiently precise and there are effective safeguards against abuse or misuse, including oversight and review by an independent and impartial tribunal or regulatory body. However, he is also concerned that States frequently rely heavily on blocking measures, rather than focusing their efforts on prosecuting those responsible for the production and dissemination of child pornography. Additionally, as child pornography is often a by-product of trafficking and prostitution of children, the Special Rapporteur urges States to take holistic measures to combat the root problems that give rise to child pornography.

B. Criminalization of legitimate expression

33. The types of action taken by States to limit the dissemination of content online not only include measures to prevent information from reaching the end-user, but also direct targeting of those who seek, receive and impart politically sensitive information via the Internet. Physically silencing criticism or dissent through arbitrary arrests and detention, enforced disappearance, harassment and intimidation is an old phenomenon, and also applies to Internet users. This issue has been explored in the Special Rapporteur's report to the General Assembly under the section on "protection of citizen journalists" (A/65/284). Such actions are often aimed not only to silence legitimate expression, but also to intimidate a population to push its members towards self-censorship.

34. The Special Rapporteur remains concerned that legitimate online expression is being criminalized in contravention of States' international human rights obligations, whether it is through the application of existing criminal laws to online expression, or through the creation of new laws specifically designed to criminalize expression on the Internet. Such laws are often justified on the basis of protecting an individual's reputation, national security or countering terrorism, but in practice are used to censor content that the Government and other powerful entities do not like or agree with.

35. One clear example of criminalizing legitimate expression is the imprisonment of bloggers around the world. According to Reporters without Borders, in 2010, 109 bloggers were in prison on charges related to the content of their online expression.[16] Seventy-two

[16] Available from: http://en.rsf.org/press-freedom-barometer-journalists-killed.html?annee=2010.

individuals were imprisoned in China alone, followed by Viet Nam and Iran, with 17 and 13 persons respectively.[17]

36. Imprisoning individuals for seeking, receiving and imparting information and ideas can rarely be justified as a proportionate measure to achieve one of the legitimate aims under article 19, paragraph 3, of the International Covenant on Civil and Political Rights. The Special Rapporteur would like to reiterate that defamation should be decriminalized, and that protection of national security or countering terrorism cannot be used to justify restricting the right to expression unless the Government can demonstrate that: (a) the expression is intended to incite imminent violence; (b) it is likely to incite such violence; and (c) there is a direct and immediate connection between the expression and the likelihood or occurrence of such violence.[18]

37. Additionally, the Special Rapporteur reiterates that the right to freedom of expression includes expression of views and opinions that offend, shock or disturb. Moreover, as the Human Rights Council has also stated in its resolution 12/16, restrictions should never be applied, inter alia, to discussion of Government policies and political debate; reporting on human rights, Government activities and corruption in Government; engaging in election campaigns, peaceful demonstrations or political activities, including for peace or democracy; and expression of opinion and dissent, religion or belief, including by persons belonging to minorities or vulnerable groups.[19]

C. Imposition of intermediary liability

38. One of the unique features of the Internet is that the way in which information is transmitted largely depends on intermediaries, or private corporations which provide services and platforms that facilitate online communication or transactions between third parties, including giving access to, hosting, transmitting and indexing content.[20] Intermediaries thus range from Internet service providers (ISPs) to search engines, and from blogging services to online community platforms. With the advent of Web 2.0 services, individuals can now publish information without the centralized gateway of editorial review common in traditional publication formats. The range of services offered by intermediaries has flourished over the past decade, mainly due to the legal protection that they have enjoyed from liability for third-party content that Internet users send via their services. However, the Special Rapporteur notes that in recent years, intermediaries' protection from liability has been eroding.

39. Many States have adopted laws which impose liability upon intermediaries if they do not filter, remove or block content generated by users which is deemed illegal. For example, in Turkey, Law 5651 on the Prevention of Crime Committed in the Information Technology Domain, which was enacted in 2007, imposes new obligations on content providers, ISPs and website hosts. It also grants authority to an agency to issue administrative orders to block websites for content hosted outside of Turkey, and to take down eight broad types of unlawful content,[21] including "crimes against Ataturk", which

[17] Reporters without Borders, "Enemies of the Internet," March 2010. Available from: http://en.rsf.org/IMG/pdf/Internet_enemies.pdf.

[18] Johannesburg Principles on National Security, Freedom of Expression and Access to Information, Principle 6, as endorsed in E/CN.4/1996/39.

[19] Human Rights Council resolution 12/16, para. 5(p).

[20] Organisation for Economic Cooperation and Development, *The Economic and Social Role of Internet Intermediaries* (April 2010).

[21] Law 5651, art. 8.

includes "insulting" the founder of the Republic of Turkey, Mustafa Kemal Ataturk. In Thailand, the 2007 Computer Crimes Act imposes liability upon intermediaries that transmit or host third-party content and content authors themselves.[22] This law has been used to prosecute individuals providing online platforms, some of which are summarized in the first addendum.

40. In other cases, intermediary liability is imposed through privacy and data protection laws. For example, a court in Italy convicted three Google executives for violating the Italian data protection code after a video depicting cruelty to a disabled teenager was posted by a user on the Google video service. Even though the video was taken down within hours of notification by Italian law enforcers, the judge found the Google executives guilty.[23] The Government of China requires ISPs and web platforms to conduct surveillance on their users, and they are also held directly responsible for content posted by users.[24] Companies that fail to comply with this obligation risk losing their business licences. Holding intermediaries liable for the content disseminated or created by their users severely undermines the enjoyment of the right to freedom of opinion and expression, because it leads to self-protective and over-broad private censorship, often without transparency and the due process of the law.

41. Several States have sought to protect intermediaries through adopting variations on what is known as a "notice-and-takedown" regime. Such a system protects intermediaries from liability, provided that they take down unlawful material when they are made aware of its existence. For example, under the European Union-wide E-Commerce Directive, a provider of hosting services for user-generated content can avoid liability for such content if it does not have actual knowledge of illegal activity and if it expeditiously removes the content in question when made aware of it.[25] Similarly, the Digital Millennium Copyright Act of the United States of America also provides safe harbour for intermediaries, provided that they take down the content in question promptly after notification.[26]

42. However, while a notice-and-takedown system is one way to prevent intermediaries from actively engaging in or encouraging unlawful behaviour on their services, it is subject to abuse by both State and private actors. Users who are notified by the service provider that their content has been flagged as unlawful often have little recourse or few resources to challenge the takedown.[27] Moreover, given that intermediaries may still be held financially or in some cases criminally liable if they do not remove content upon receipt of notification by users regarding unlawful content, they are inclined to err on the side of safety by over-censoring potentially illegal content. Lack of transparency in the intermediaries' decision-making process also often obscures discriminatory practices or political pressure affecting the companies' decisions. Furthermore, intermediaries, as private entities, are not best placed to make the determination of whether a particular content is illegal, which requires careful balancing of competing interests and consideration of defences.

[22] Computer Crimes Act B.E.2550 (2007), sections 14 and 15.

[23] Reporters without Borders, "Google conviction could lead to prior control over videos posted online", 24 February 2010.

[24] Reporters without Borders, "Enemies of the Internet," March 2010. Available from: http://en.rsf.org/IMG/pdf/Internet_enemies.pdf, pp. 8-12.

[25] E/Commerce Directive, 2000/31/EC, art. 14.

[26] Digital Millennium Copyright Act, Section 512.

[27] N. Villeneuve, "Evasion Tactics: Global Online Censorship is Growing, but so are the Means to challenge it and Protect Privacy", *Index on Censorship* Vol. 36 No. 4, (November 2007); Center for Democracy and Technology, "Campaign takedown troubles: how meritless copyright claims threaten online political speech" (September 2010).

43. The Special Rapporteur believes that censorship measures should never be delegated to a private entity, and that no one should be held liable for content on the Internet of which they are not the author. Indeed, no State should use or force intermediaries to undertake censorship on its behalf, as is the case in the Republic of Korea with the establishment of the Korea Communications Standards Commission, a quasi-State and quasi-private entity tasked to regulate online content (see A/HRC/17/27/Add.2). The Special Rapporteur welcomes initiatives taken in other countries to protect intermediaries, such as the bill adopted in Chile, which provides that intermediaries are not required to prevent or remove access to user-generated content that infringes copyright laws until they are notified by a court order. [28] A similar regime has also been proposed in Brazil.[29]

Responsibility of intermediaries

44. Given that Internet services are run and maintained by private companies, the private sector has gained unprecedented influence over individuals' right to freedom of expression and access to information. Generally, companies have played an extremely positive role in facilitating the exercise of the right to freedom of opinion and expression. At the same time, given the pressure exerted upon them by States, coupled with the fact that their primary motive is to generate profit rather than to respect human rights, preventing the private sector from assisting or being complicit in human rights violations of States is essential to guarantee the right to freedom of expression.

45. While States are the duty-bearers for human rights, private actors and business enterprises also have a responsibility to respect human rights. In this regard, the Special Rapporteur highlights the framework of "Protect, Respect and Remedy" which has been developed by the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises. The framework rests on three pillars: (a) the duty of the State to protect against human rights abuses by third parties, including business enterprises, through appropriate policies, regulation and adjudication; (b) the corporate responsibility to respect human rights, which means that business enterprises should act with due diligence to avoid infringing the rights of others and to address adverse impacts with which they are involved; and (c) the need for greater access by victims to effective remedy, both judicial and non-judicial.[30]

46. The Special Rapporteur notes that multi-stakeholder initiatives are essential to deal effectively with issues related to the Internet, and the Global Network Initiative serves as a helpful example to encourage good practice by corporations.[31] Although only three corporations, namely Google, Microsoft, and Yahoo!, have participated in this initiative so far, the Special Rapporteur welcomes their commitment to undertake a human rights impact assessment of their decisions, including before entering a foreign market, and to ensure transparency and accountability when confronted with situations that may undermine the rights to freedom of expression and privacy. Google's Transparency Report[32] is an outcome of such work, and provides information on Government inquiries for information about users and requests for Google to take down or censor content, as well as statistical information on traffic to Google services, such as YouTube. By illustrating traffic patterns for a given country or region, it allows users to discern any disruption in the free flow of information, whether it is due to Government censorship or a cable cut.

[28] Ley No. 20435, Modifica La Ley No.17.336 Sobre Propiedad Intelectual, chap. III, art. 85-L – art. 85-U, adopted on 4 May 2010.

[29] "New Draft Bill Proposition: Available for Download", Marco Civil da Internet, 21 May 2010.

[30] A/HRC/17/31, para. 6.

[31] See http://www.globalnetworkinitiative.org/principles/index.php.

[32] See www.google.com/transparencyreport.

47. The Special Rapporteur commends such initiatives to enhance the responsibility of Internet intermediaries to respect human rights. To avoid infringing the right to freedom of expression and the right to privacy of Internet users, the Special Rapporteur recommends intermediaries to: only implement restrictions to these rights after judicial intervention; be transparent to the user involved about measures taken, and where applicable to the wider public; provide, if possible, forewarning to users before the implementation of restrictive measures; and minimize the impact of restrictions strictly to the content involved. Finally, there must be effective remedies for affected users, including the possibility of appeal through the procedures provided by the intermediary and by a competent judicial authority.

48. More generally, the Special Rapporteur encourages corporations to establish clear and unambiguous terms of service in line with international human rights norms and principles, increase transparency of and accountability for their activities, and continuously review the impact of their services and technologies on the right to freedom of expression of their users, as well as on the potential pitfalls involved when they are misused.

D. Disconnecting users from Internet access, including on the basis of violations of intellectual property rights law

49. While blocking and filtering measures deny access to certain content on the Internet, States have also taken measures to cut off access to the Internet entirely. The Special Rapporteur is deeply concerned by discussions regarding a centralized "on/off" control over Internet traffic.[33] In addition, he is alarmed by proposals to disconnect users from Internet access if they violate intellectual property rights. This also includes legislation based on the concept of "graduated response", which imposes a series of penalties on copyright infringers that could lead to suspension of Internet service, such as the so-called "three-strikes-law" in France[34] and the Digital Economy Act 2010 of the United Kingdom.[35]

50. Beyond the national level, the Anti-Counterfeiting Trade Agreement (ACTA) has been proposed as a multilateral agreement to establish international standards on intellectual property rights enforcement. While the provisions to disconnect individuals from Internet access for violating the treaty have been removed from the final text of December 2010, the Special Rapporteur remains watchful about the treaty's eventual implications for intermediary liability and the right to freedom of expression.

E. Cyber-attacks

51. Cyber-attacks, or attempts to undermine or compromise the function of a computer-based system, include measures such as hacking into accounts or computer networks, and often take the form of distributed denial of service (DDoS) attacks. During such attacks, a group of computers is used to inundate a web server where the targeted website is hosted with requests, and as a result, the targeted website crashes and becomes inaccessible for a certain period of time. As with timed blocking, such attacks are sometimes undertaken during key political moments. The Special Rapporteur also notes that websites of human

[33] "Reaching for the kill switch", *The Economist*, 10 February 2011.

[34] Decision 2009-580, Act furthering the diffusion and protection of creation on the Internet, (original: Loi favorisant la diffusion et la protection de la création sur internet), Conseil Constitutionnel, 10 June 2010. Available from: http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank_mm/anglais/2009_580dc.pdf.

[35] Digital Economy Act 2010, sections 3-16.

rights organizations and dissidents are frequently and increasingly becoming targets of DDoS attacks, some of which are included in the first addendum to this report.

52. When a cyber-attack can be attributed to the State, it clearly constitutes inter alia a violation of its obligation to respect the right to freedom of opinion and expression. Although determining the origin of cyber-attacks and the identity of the perpetrator is often technically difficult, it should be noted that States have an obligation to protect individuals against interference by third parties that undermines the enjoyment of the right to freedom of opinion and expression. This positive obligation to protect entails that States must take appropriate and effective measures to investigate actions taken by third parties, hold the persons responsible to account, and adopt measures to prevent such recurrence in the future.

F. Inadequate protection of the right to privacy and data protection

53. The right to privacy is essential for individuals to express themselves freely. Indeed, throughout history, people's willingness to engage in debate on controversial subjects in the public sphere has always been linked to possibilities for doing so anonymously. The Internet allows individuals to access information and to engage in public debate without having to reveal their real identities, for example through the use of pseudonyms on message boards and chat forums. Yet, at the same time, the Internet also presents new tools and mechanisms through which both State and private actors can monitor and collect information about individuals' communications and activities on the Internet. Such practices can constitute a violation of the Internet users' right to privacy, and, by undermining people's confidence and security on the Internet, impede the free flow of information and ideas online.

54. The Special Rapporteur is deeply concerned by actions taken by States against individuals communicating via the Internet, frequently justified broadly as being necessary to protect national security or to combat terrorism. While such ends can be legitimate under international human rights law, surveillance often takes place for political, rather than security reasons in an arbitrary and covert manner. For example, States have used popular social networking sites, such as Facebook, to identify and to track the activities of human rights defenders and opposition members, and in some cases have collected usernames and passwords to access private communications of Facebook users.

55. A number of States are also introducing laws or modifying existing laws to increase their power to monitor Internet users' activities and content of communication without providing sufficient guarantees against abuse. In addition, several States have established a real-name identification system before users can post comments or upload content online, which can compromise their ability to express themselves anonymously, particularly in countries where human rights are frequently violated. Furthermore, steps are also being taken in many countries to reduce the ability of Internet users to protect themselves from arbitrary surveillance, such as limiting the use of encryption technologies.

56. The Special Rapporteur also notes that there are insufficient or inadequate data protection laws in many States stipulating who is allowed to access personal data, what it can be used for, how it should be stored, and for how long. The necessity of adopting clear laws to protect personal data is further increased in the current information age, where large volumes of personal data are collected and stored by intermediaries, and there is a worrying trend of States obliging or pressuring these private actors to hand over information of their users. Moreover, with the increasing use of cloud-computing services, where information is stored on servers distributed in different geographical locations, ensuring that third parties also adhere to strict data protection guarantees is paramount.

57. The right to privacy is guaranteed by article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights. The latter provides that "(1) no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation; (2) everyone has the right to the protection of the law against such interference or attacks." Although "correspondence" primarily has been interpreted as written letters, this term today covers all forms of communication, including via the Internet.[36] The right to private correspondence thus gives rise to a comprehensive obligation on the part of the State to ensure that e-mails and other forms of online communication are actually delivered to the desired recipient without interference or inspection by State organs or by third parties.[37]

58. In addition, the protection of personal data represents a special form of respect for the right to privacy.[38] States parties are required by article 17(2) to regulate, through clearly articulated laws, the recording, processing, use and conveyance of automated personal data and to protect those affected against misuse by State organs as well as private parties. In addition to prohibiting data processing for purposes that are incompatible with the Covenant, data protection laws must establish rights to information, correction and, if need be, deletion of data and provide effective supervisory measures. Moreover, as stated in the Human Rights Committee's general comment on the right to privacy, "in order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files."[39]

59. The Special Rapporteur notes that the right to privacy can be subject to restrictions or limitations under certain exceptional circumstances. This may include State surveillance measures for the purposes of administration of criminal justice, prevention of crime or combating terrorism. However, such interference is permissible only if the criteria for permissible limitations under international human rights law are met. Hence, there must be a law that clearly outlines the conditions whereby individuals' right to privacy can be restricted under exceptional circumstances, and measures encroaching upon this right must be taken on the basis of a specific decision by a State authority expressly empowered by law to do so, usually the judiciary, for the purpose of protecting the rights of others, for example to secure evidence to prevent the commission of a crime, and must respect the principle of proportionality.[40]

V. Access to the Internet and the necessary infrastructure

60. The Internet, as a medium by which the right to freedom of expression can be exercised, can only serve its purpose if States assume their commitment to develop effective policies to attain universal access to the Internet. Without concrete policies and

[36] Manfred Nowak, *UN Covenant on Civil and Political Rights. CCPR Commentary* (Kehl am Rhein, Engel, 2005), p. 401.

[37] Ibid.

[38] Ibid.

[39] Human Rights Committee, general comment No. 16 on article 17 of the International Covenant on Civil and Political Rights, para. 10.

[40] Manfred Nowak, *UN Covenant on Civil and Political Rights. CCPR Commentary* (Kehl am Rhein, Engel, 2005), pp. 401-402.

plans of action, the Internet will become a technological tool that is accessible only to a certain elite while perpetrating the "digital divide".

61. The term "digital divide" refers to the gap between people with effective access to digital and information technologies, in particular the Internet, and those with very limited or no access at all. In contrast to 71.6 Internet users per 100 inhabitants in developed States, there are only 21.1 Internet users per 100 inhabitants in developing States.[41] This disparity is starker in the African region, with only 9.6 users per 100 inhabitants.[42] In addition, digital divides also exist along wealth, gender, geographical and social lines within States. Indeed, with wealth being one of the significant factors in determining who can access information communication technologies, Internet access is likely to be concentrated among socio-economic elites, particularly in countries where Internet penetration is low. In addition, people in rural areas are often confronted with obstacles to Internet access, such as lack of technological availability, slower Internet connection, and/or higher costs. Furthermore, even where Internet connection is available, disadvantaged groups, such as persons with disabilities and persons belonging to minority groups, often face barriers to accessing the Internet in a way that is meaningful, relevant and useful to them in their daily lives.

62. The Special Rapporteur is thus concerned that without Internet access, which facilitates economic development and the enjoyment of a range of human rights, marginalized groups and developing States remain trapped in a disadvantaged situation, thereby perpetuating inequality both within and between States. As he has noted previously, to combat situations of inequality it is critical to ensure that marginalized or disadvantaged sections of society can express their grievances effectively and that their voices are heard. [43] The Internet offers a key means by which such groups can obtain information, assert their rights, and participate in public debates concerning social, economic and political changes to improve their situation. Moreover, the Internet is an important educational tool, as it provides access to a vast and expanding source of knowledge, supplements or transforms traditional forms of schooling, and makes, through "open access" initiatives, previously unaffordable scholarly research available to people in developing States. Additionally, the educational benefits attained from Internet usage directly contribute to the human capital of States.

63. The Special Rapporteur notes that several initiatives have been taken in an attempt to bridge the digital divide. At the international level, Target 8f of the Millennium Development Goals calls upon States, "in consultation with the private sector, [to] make available the benefits of new technologies, especially information and communications." The necessity of achieving this target was reiterated in the 2003 Plan of Action adopted at the Geneva World Summit on the Information Society, which outlines specific goals and targets to "build an inclusive Information Society; to put the potential of knowledge and [information communication technologies] (ICTs) at the service of development; to promote the use of information and knowledge for the achievement of internationally agreed development goals."[44] To implement this plan of action, in 2005, the International Telecommunication Union launched the "Connect the World" project.[45] Another initiative to spread the availability of ICTs in developing countries is the "One Laptop Per Child"

[41] "Key Global Telecom Indicators for the World Telecommunication Service Sector," International Telecommunication Union, 21 October 2010.

[42] Ibid.

[43] See A/HRC/14/23.

[44] WSIS-03/GENEVA/DOC/5-E, World Summit on the Information Society, 12 December 2003. Available from: http://www.itu.int/wsis/docs/geneva/official/poa.html.

[45] "Connect the World," International Telecommunication Union. Available from: http://www.itu.int/ITU-D/connect.

project that has been supported by the United Nations Development Programme. This project distributes affordable laptops that are specifically customized for the learning environment of children. Since this project was mentioned in the previous mandate holder's report in 2006, 2.4 million laptops have been distributed to children and teachers worldwide.[46] In Uruguay, the project has reached 480,000 children, amounting to almost all children enrolled in primary school.[47] States in Africa lag behind, but in Rwanda, over 56,000 laptops have been distributed, with plans for the figure to reach 100,000 by June 2011.[48]

64. At the national level, the Special Rapporteur notes that a number of initiatives have also been taken by States to address the digital divide. In India, Common Service Centres, or public "e-Kiosks", have been established by the Government in collaboration with the private sector as part of the National E-Governance Plan of 2006. As of January 2011, over 87,000 centres have reportedly been established,[49] although the Special Rapporteur notes that the majority of the country's population still remains without Internet access. In Brazil, the Government has launched a "computers for all" programme which offers subsidies for purchasing computers.[50] Additionally, over 100,000 publicly sponsored Internet access centres, known as "Local Area Network (LAN) Houses" with fast broadband Internet connections, have been established.[51] Such public access points are particularly important to facilitate access for the poorest socio-economic groups, as they often do not have their own personal computers at home.

65. In some economically developed States, Internet access has been recognized as a right. For example, the parliament of Estonia passed legislation in 2000 declaring Internet access a basic human right.[52] The constitutional council of France effectively declared Internet access a fundamental right in 2009, and the constitutional court of Costa Rica reached a similar decision in 2010.[53] Going a step further, Finland passed a decree in 2009 stating that every Internet connection needs to have a speed of at least one Megabit per second (broadband level).[54] The Special Rapporteur also takes note that according to a

[46] E/CN.4/2006/55, 30 December 2005, para. 34; "Map," One Laptop per Child. Available from: http://one.laptop.org/map.

[47] Available from: http://laptop.org/en/children/countries/index.shtml.

[48] Frank Kanyesigye, "OLPC Extends to Over 100 Schools," New Times, 11 February 2011. Available from: http://www.newtimes.co.rw/index.php?issue=14533&article=38241.

[49] "ICT Ministers meet tomorrow for speeding-up delivery of e-services," Press Information Bureau, Government of India, 26 October 2009; and "E-Governance Initiatives-Changing Lives for the better," Press Information Bureau, Government of India, 24 January 2011. Available from: http://pib.nic.in/newsite/erelease.aspx?relid=69324.

[50] Ronaldo Lemos and Paula Martini, "LAN Houses: A new wave of digital inclusion in Brazil", 21 September 2009. Available from: http://publius.cc/lan_houses_new_wave_digital_inclusion_brazil/091509.

[51] Ibid.

[52] Colin Woodard, "Estonia, where being wired is a human right," Christian Science Monitor, 1 July 2003.

[53] Decision 2009-580, Act furthering the diffusion and protection of creation on the Internet.

[54] "732/2009, Decree of the Ministry of Transport and Communications on the minimum rate of a functional Internet access as a universal service," (original: Liikenne- ja viestintäministeriön asetus tarkoituksenmukaisen internet-yhtyeden vähimmäisnopeudesta yleispalvelussa), FINLEX, 22 October 2009. Available from: http://www.finlex.fi/en/laki/kaannokset/2009/en20090732.

survey by the British Broadcasting Corporation in March 2010, 79% of those interviewed in 26 countries believe that Internet access is a fundamental human right.[55]

66. Given that access to basic commodities such as electricity remains difficult in many developing States, the Special Rapporteur is acutely aware that universal access to the Internet for all individuals worldwide cannot be achieved instantly. However, the Special Rapporteur reminds all States of their positive obligation to promote or to facilitate the enjoyment of the right to freedom of expression and the means necessary to exercise this right, including the Internet. Hence, States should adopt effective and concrete policies and strategies – developed in consultation with individuals from all segments of society, including the private sector as well as relevant Government ministries – to make the Internet widely available, accessible and affordable to all.

VI. Conclusions and recommendations

67. **Unlike any other medium, the Internet enables individuals to seek, receive and impart information and ideas of all kinds instantaneously and inexpensively across national borders. By vastly expanding the capacity of individuals to enjoy their right to freedom of opinion and expression, which is an "enabler" of other human rights, the Internet boosts economic, social and political development, and contributes to the progress of humankind as a whole. In this regard, the Special Rapporteur encourages other Special Procedures mandate holders to engage on the issue of the Internet with respect to their particular mandates.**

68. **The Special Rapporteur emphasizes that there should be as little restriction as possible to the flow of information via the Internet, except in few, exceptional, and limited circumstances prescribed by international human rights law. He also stresses that the full guarantee of the right to freedom of expression must be the norm, and any limitation considered as an exception, and that this principle should never be reversed. Against this backdrop, the Special Rapporteur recommends the steps set out below.**

A. Restriction of content on the Internet

69. **The Special Rapporteur is cognizant of the fact that, like all technological inventions, the Internet can be misused to cause harm to others. As with offline content, when a restriction is imposed as an exceptional measure on online content, it must pass a three-part, cumulative test: (1) it must be provided by law, which is clear and accessible to everyone (principles of predictability and transparency); (2) it must pursue one of the purposes set out in article 19, paragraph 3, of the International Covenant on Civil and Political Rights , namely: (i) to protect the rights or reputations of others; (ii) to protect national security or public order, or public health or morals (principle of legitimacy); and (3) it must be proven as necessary and the least restrictive means required to achieve the purported aim (principles of necessity and proportionality). In addition, any legislation restricting the right to freedom of expression must be applied by a body which is independent of any political, commercial, or other unwarranted influences in a manner that is neither arbitrary nor discriminatory. There should also be adequate safeguards against abuse, including the possibility of challenge and remedy against its abusive application.**

[55] "Four in five regard Internet access as a fundamental right: global poll," BBC News, 8 March 2010. Available from: http://news.bbc.co.uk/1/shared/bsp/hi/pdfs/08_03_10_BBC_internet_poll.pdf.

1. Arbitrary blocking or filtering of content on the Internet

70. **The Special Rapporteur is deeply concerned by increasingly sophisticated blocking or filtering mechanisms used by States for censorship. The lack of transparency surrounding these measures also makes it difficult to ascertain whether blocking or filtering is really necessary for the purported aims put forward by States. As such, the Special Rapporteur calls upon States that currently block websites to provide lists of blocked websites and full details regarding the necessity and justification for blocking each individual website. An explanation should also be provided on the affected websites as to why they have been blocked. Any determination on what content should be blocked must be undertaken by a competent judicial authority or a body which is independent of any political, commercial, or other unwarranted influences.**

71. **With regard to child pornography, the Special Rapporteur notes that it is one clear exception where blocking measures are justified, provided that the national law is sufficiently precise and there are sufficient safeguards against abuse or misuse to prevent any "mission creep", including oversight and review by an independent and impartial tribunal or regulatory body. However, the Special Rapporteur calls upon States to focus their efforts on prosecuting those responsible for the production and dissemination of child pornography, rather than on blocking measures alone.**

2. Criminalization of legitimate expression

72. **The Special Rapporteur remains concerned that legitimate online expression is being criminalized in contravention of States' international human rights obligations, whether it is through the application of existing criminal laws to online expression, or through the creation of new laws specifically designed to criminalize expression on the Internet. Such laws are often justified as being necessary to protect individuals' reputation, national security or to counter terrorism. However, in practice, they are frequently used to censor content that the Government and other powerful entities do not like or agree with.**

73. **The Special Rapporteur reiterates the call to all States to decriminalize defamation. Additionally, he underscores that protection of national security or countering terrorism cannot be used to justify restricting the right to expression unless it can be demonstrated that: (a) the expression is intended to incite imminent violence; (b) it is likely to incite such violence; and (c) there is a direct and immediate connection between the expression and the likelihood or occurrence of such violence.**

3. Imposition of intermediary liability

74. **Intermediaries play a fundamental role in enabling Internet users to enjoy their right to freedom of expression and access to information. Given their unprecedented influence over how and what is circulated on the Internet, States have increasingly sought to exert control over them and to hold them legally liable for failing to prevent access to content deemed to be illegal.**

75. **The Special Rapporteur emphasizes that censorship measures should never be delegated to private entities, and that intermediaries should not be held liable for refusing to take action that infringes individuals' human rights. Any requests submitted to intermediaries to prevent access to certain content, or to disclose private information for strictly limited purposes such as administration of criminal justice, should be done through an order issued by a court or a competent body which is independent of any political, commercial or other unwarranted influences.**

76. **In addition, while States are the primary duty-bearers of human rights, the Special Rapporteur underscores that corporations also have a responsibility to respect human rights, which means that they should act with due diligence to avoid infringing the rights of individuals. The Special Rapporteur thus recommends intermediaries to: only implement restrictions to these rights after judicial intervention; be transparent to the user involved about measures taken, and, where applicable, to the wider public; provide, if possible, forewarning to users before the implementation of restrictive measures; and minimize the impact of restrictions strictly to the content involved. Finally, there must be effective remedies for affected users, including the possibility of appeal through the procedures provided by the intermediary and by a competent judicial authority.**

77. **The Special Rapporteur commends the work undertaken by organizations and individuals to reveal the worldwide status of online impediments to the right to freedom of expression. He encourages intermediaries in particular to disclose details regarding content removal requests and accessibility of websites. Additionally, he recommends corporations to establish clear and unambiguous terms of service in line with international human rights norms and principles and to continuously review the impact of their services and technologies on the right to freedom of expression of their users, as well as on the potential pitfalls involved when they are misused. The Special Rapporteur believes that such transparency will help promote greater accountability and respect for human rights.**

4. Disconnecting users from Internet access, including on the basis of intellectual property rights law

78. **While blocking and filtering measures deny users access to specific content on the Internet, States have also taken measures to cut off access to the Internet entirely. The Special Rapporteur considers cutting off users from Internet access, regardless of the justification provided, including on the grounds of violating intellectual property rights law, to be disproportionate and thus a violation of article 19, paragraph 3, of the International Covenant on Civil and Political Rights.**

79. **The Special Rapporteur calls upon all States to ensure that Internet access is maintained at all times, including during times of political unrest. In particular, the Special Rapporteur urges States to repeal or amend existing intellectual copyright laws which permit users to be disconnected from Internet access, and to refrain from adopting such laws.**

5. Cyber-attacks

80. **The Special Rapporteur is deeply concerned that websites of human rights organizations, critical bloggers, and other individuals or organizations that disseminate information that is embarrassing to the State or the powerful have increasingly become targets of cyber-attacks.**

81. **When a cyber-attack can be attributed to the State, it clearly constitutes, inter alia, a violation of its obligation to respect the right to freedom of opinion and expression. Although determining the origin of cyber-attacks and the identity of the perpetrator is often technically difficult, it should be noted that States have an obligation to protect individuals against interference by third parties that undermines the enjoyment of the right to freedom of opinion and expression. This positive obligation to protect entails that States must take appropriate and effective measures to investigate actions taken by third parties, hold the persons responsible to account, and adopt measures to prevent such recurrence in the future.**

6. Inadequate protection of the right to privacy and data protection

82. **The Special Rapporteur is concerned that, while users can enjoy relative anonymity on the Internet, States and private actors have access to technology to monitor and collect information about individuals' communications and activities on the Internet. Such practices can constitute a violation of Internet users' right to privacy, and undermine people's confidence and security on the Internet, thus impeding the free flow of information and ideas online.**

83. **The Special Rapporteur underscores the obligation of States to adopt effective privacy and data protection laws in accordance with article 17 of the International Covenant on Civil and Political Rights and the Human Rights Committee's general comment No. 16. This includes laws that clearly guarantee the right of all individuals to ascertain in an intelligible form whether, and if so what, personal data is stored in automatic data files, and for what purposes, and which public authorities or private individuals or bodies control or may control their files.**

84. **He also calls upon States to ensure that individuals can express themselves anonymously online and to refrain from adopting real-name registration systems. Under certain exceptional situations where States may limit the right to privacy for the purposes of administration of criminal justice or prevention of crime, the Special Rapporteur underscores that such measures must be in compliance with the international human rights framework, with adequate safeguards against abuse. This includes ensuring that any measure to limit the right to privacy is taken on the basis of a specific decision by a State authority expressly empowered by law to do so, and must respect the principles of necessity and proportionality.**

B. Access to the Internet and the necessary infrastructure

85. **Given that the Internet has become an indispensable tool for realizing a range of human rights, combating inequality, and accelerating development and human progress, ensuring universal access to the Internet should be a priority for all States. Each State should thus develop a concrete and effective policy, in consultation with individuals from all sections of society, including the private sector and relevant Government ministries, to make the Internet widely available, accessible and affordable to all segments of population.**

86. **At the international level, the Special Rapporteur reiterates his call on States, in particular developed States, to honour their commitment, expressed inter alia in the Millennium Development Goals, to facilitate technology transfer to developing States, and to integrate effective programmes to facilitate universal Internet access in their development and assistance policies.**

87. **Where the infrastructure for Internet access is present, the Special Rapporteur encourages States to support initiatives to ensure that online information can be accessed in a meaningful way by all sectors of the population, including persons with disabilities and persons belonging to linguistic minorities.**

88. **States should include Internet literacy skills in school curricula, and support similar learning modules outside of schools. In addition to basic skills training, modules should clarify the benefits of accessing information online, and of responsibly contributing information. Training can also help individuals learn how to protect themselves against harmful content, and explain the potential consequences of revealing private information on the Internet.**