NATIONS UNIES
DROITS DE L'HOMME
HAUT-COMMISSARIAT

UNITED NATIONS
HUMAN RIGHTS
OFFICE OF THE HIGH COMMISSIONER

HAUT-COMMISSARIAT AUX DROITS DE L'HOMME • OFFICE OF THE HIGH COMMISSIONER FOR HUMAN RIGHTS
PALAIS DES NATIONS • 1211 GENEVA 10, SWITZERLAND
www.ohchr.org • TEL: +41 22 917 9000 • FAX: +41 22 917 9008 • E-MAIL: registry@ohchr.org

Contributions by the Office of the High Commissioner for Human Rights to UNESCO's Comprehensive Study on Internet-related Issues

INTRODUCTION

The Office of the High Commissioner for Human Rights is pleased to present its contributions to UNESCO Comprehensive Study on Internet-related Issues.

These contributions have been extracted from published reports by the High Commissioner for Human Rights and relevant Special Rapporteurs, as detailed in the "Reference Documents" section of this document. The source of each excerpt is indicated in a footnote. For further information or to obtain additional context, the full reports should be consulted.

REPLIES TO THE QUESTIONNAIRE

A. Questions related to the field of Access to information and knowledge

- **Question (1)**: *What can be done to reinforce the right to seek and receive information in the online environment?*

- "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 plans of action, the Internet will become a technological tool that is accessible only to a certain elite while perpetrating the "digital divide"."[1]

- "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

[1] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, Report of the Special Rapporteur to the Human Rights Council on key trends and challenges to the right of all individuals to seek, receive and impart information and ideas of all kinds through the Internet, *UN Doc. A/HRC/17/27*, 16 May 2011, para. 60.

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." To implement this plan of action, in 2005, the International Telecommunication Union launched the "Connect the World" project. Another initiative to spread the availability of ICTs in developing countries is the "One Laptop Per Child" 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. In Uruguay, the project has reached 480,000 children, amounting to almost all children enrolled in primary school. 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. 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, 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. Additionally, over 100,000 publicly sponsored Internet access centres, known as "Local Area Network (LAN) Houses" with fast broadband Internet connections, have been established. 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. 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. 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. 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). The Special Rapporteur also takes note that according to a 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."[2]

- "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. 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." "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."[3]

- "In addition to the availability of relevant content online which is free of censorship, the Special Rapporteur also notes the importance of ensuring that individuals possess the necessary skills to make full use of the Internet, or what is often referred to as "digital literacy". The Special Rapporteur encourages States to provide support for training in information and communications technology (ICT) skills, which can range from basic computer skills to creating web pages. In terms of the right to freedom of expression, course modules should not only clarify the benefits of accessing information online, but also of responsibly contributing information, which can also contribute to combating the third type of expression mentioned above."[4]

- "[…] given that the Internet has become an indispensable tool for full participation in political, cultural, social and economic life, States should adopt effective and concrete

[2] Report of the Special Rapporteur to the Human Rights Council on key trends and challenges to the right of all individuals to seek, receive and impart information and ideas of all kinds through the Internet, *supra*, paras. 63, 64, 65.
[3] Report of the Special Rapporteur to the Human Rights Council on key trends and challenges to the right of all individuals to seek, receive and impart information and ideas of all kinds through the Internet, *supra*, paras. 85, 86, 88.
[4] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Report of the Special Rapporteur to the General Assembly on the right to freedom of opinion and expression exercised through the Internet, *UN Doc. A/66/290,* 10 August 2011, para. 45.

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."[5]

- "In particular, the Special Rapporteur recommends that States take proactive measures to ensure that Internet connectivity is available on an individual or communal level in all inhabited localities of the State, by working on initiatives with the private sector, including in remote or rural areas. Such measures involve the adoption and implementation of policies that facilitate access to Internet connection and to low-cost hardware, including in remote and rural areas, including the subsidization of service, if necessary."[6]

- **Question (3)**: *How can greater progress be made as regards inclusive strategies for women and girls as well as marginalized and disabled people?*

- "The Special Rapporteur underscores that the needs of persons with disabilities should be taken into account when designing and implementing Internet infrastructure at all levels. This can be in relation to distribution, user facilities as well as access devices. Some positive examples include the "Community Access" programme in Canada, which seeks to provide an appropriate number of sites with enhanced accessibility to meet the broad range of needs of persons with disabilities. The programme also aims to provide Internet access to less likely users, such as individuals with low incomes, rural or Aboriginal population, the elderly and immigrants. In the United States of America, the Senate unanimously passed the "Twenty-first Century Communications and Video Accessibility Act" in 2010. The Act seeks to ensure full access for users who are deaf, hard of hearing, late deafened or deaf-blind to evolving high-speed broadband, wireless and other Internet protocol technologies. Moreover, the Act stipulates that accessibility features are preserved when materials are offered online, that telephones used over the Internet must be compatible with hearing aids and that television programmes must also be captioned when delivered over the Internet." "The United Nations Girls' Education Initiative, evolving from the Millennium Villages project, is an example of "e-education" initiatives which also help promote girls' education. This initiative has launched a global campaign to promote universal and equality Internet access in secondary education in developing countries, with

[5] Report of the Special Rapporteur to the General Assembly on the right to freedom of opinion and expression exercised through the Internet, *supra*, para. 63.
[6] Report of the Special Rapporteur to the General Assembly on the right to freedom of opinion and expression exercised through the Internet, *supra*, para. 89.

an emphasis on girls' education. ICT skills will be used to enhance the quality of education and to connect schoolchildren worldwide."[7]

- **Question (4)**: *How can accessibility be facilitated through increases in locally produced and relevant content in different languages?*

- "Other positive initiatives to overcome language barriers include, for example, the World Digital Library, which provides free, multilingual access to documentary heritage held in institutions around the world, aimed at a diverse audience, from students, teachers to ordinary members of the public. Furthermore, the content is contributed by partner institutions in the language of origin and is accessed through an interactive interface in seven languages, and allows for voice enabled browsing and can allow easy access to people with visual disabilities. The Special Rapporteur also notes that the Board of the Internet Corporation for Assigned Names and Numbers has approved the internationalized domain name (IDN) ccTLD Fast Track Process, which enables countries and territories that use languages based on scripts other than Latin to offer their user's domain names in non-Latin characters."[8]

B. Questions related to the field of Freedom of Expression

- **Question (6)**: *What are the current and emerging challenges relevant to freedom of expression online?*

- "In the digital era, communications technologies also have enhanced the capacity of Governments, enterprises and individuals to conduct surveillance, interception and data collection. As noted by the Special Rapporteur on the right to freedom of expression and opinion, technological advancements mean that the State's effectiveness in conducting surveillance is no longer limited by scale or duration."[9]

- "While the mandate for the present report focused on the right to privacy, it should be underscored that other rights also may be affected by mass surveillance, the interception of

[7] Report of the Special Rapporteur to the General Assembly on the right to freedom of opinion and expression exercised through the Internet, *supra*, paras. 51,52, 59.
[8] Report of the Special Rapporteur to the General Assembly on the right to freedom of opinion and expression exercised through the Internet, *supra*, paras. 55, 56.
[9] The right to privacy in the digital age - Report of the Office of the United Nations High Commissioner for Human Rights, UN Doc. A/HRC/27/37, para. 2.

digital communications and the collection of personal data. These include the rights to freedom of opinion and expression, and to seek, receive and impart information; to freedom of peaceful assembly and association; and to family life – rights all linked closely with the right to privacy and, increasingly, exercised through digital media."[10]

- "Even the mere possibility of communications information being captured creates an interference with privacy, with a potential chilling effect on rights, including those to free expression and association."[11]

- "The significant potential of the Internet as a tool to promote the free flow of information and ideas has not been fully realized due to efforts by some governments to control or limit this medium. We are particularly concerned about: (a) The fragmentation of the Internet through the imposition of firewalls and filters, as well as through registration requirements; (b) State interventions, such as blocking of websites and web domains which give access to user-generated content or social networking, justified on social, historical or political grounds; (c) The fact that some corporations which provide Internet searching, access, chat, publishing or other services fail to make a sufficient effort to respect the rights of those who use their services to access the Internet without interference, for example on political grounds; (d) Jurisdictional rules which allow cases, particularly defamation cases, to be pursued anywhere, leading to a lowest common denominator approach."[12]

- "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."[13]

- "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

[10]The right to privacy in the digital age, *supra*, para. 14.
[11] The right to privacy in the digital age, *supra*, para. 20.
[12] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Tenth anniversary joint declaration: Ten key challenges to freedom of expression in the next decade, *UN Doc. A/HRC/14/23/Add.2*, 25 March 2010, Challenge No. 9, p. 7.
[13] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, Report of the Special Rapporteur to the Human Rights Council on key trends and challenges to the right of all individuals to seek, receive and impart information and ideas of all kinds through the Internet, *UN Doc. A/HRC/17/27*, 16 May 2011, para. 23.

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." "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." "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." "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." "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."[14]

- **Question (8)**: *Is there a need for specific protections for freedom of expression for the Internet?*

- "…, the Special Rapporteur emphasizes that due to the unique characteristics of the Internet, regulations or restrictions which may be deemed legitimate and proportionate for

[14] Report of the Special Rapporteur to the Human Rights Council on key trends and challenges to the right of all individuals to seek, receive and impart information and ideas of all kinds through the Internet, *supra*, paras. 70, 72, 74, 78, 80.

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. 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. 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."[15]

- "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." "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."[16]

- **Question (9)**: *To what extent do laws protect digitally interfaced journalism and journalistic sources?*

- "The emergence of "online journalists"–both professionals and untrained so-called "citizen journalists"–play an increasingly important role in documenting and disseminating news in real time as they unfold on the ground. Journalists who publish their work online should be afforded the same protection under articles 19 of the Universal Declaration on Human Rights and of the International Covenant on Civil and Political Rights. Any restriction

[15] Report of the Special Rapporteur to the Human Rights Council on key trends and challenges to the right of all individuals to seek, receive and impart information and ideas of all kinds through the Internet, *supra*, para. 27.
[16] Report of the Special Rapporteur to the Human Rights Council on key trends and challenges to the right of all individuals to seek, receive and impart information and ideas of all kinds through the Internet, *supra*, paras. 46, 47.

applied to online content must also be in conformity with the three-part test set out in article 19, paragraph 3, of the Covenant."[17]

- **Question (10)**: *What are the optimum ways to deal with online hate speech?*

- "… to bring about real changes in mindsets, perceptions, and discourse, a broad set of policy measures are necessary, for example in the areas of intercultural dialogue or education for diversity, equality and justice and in strengthening freedom of expression and promoting a "culture of peace". Indeed, the Special Rapporteur has previously stated that the strategic response to expressions deemed as offensive or intolerant is more speech: more speech that educates about cultural differences; more speech that promotes diversity and understanding; more speech to empower and give voice to minorities and indigenous peoples, for example through the support of community media and their representation in mainstream media. More speech can be the best strategy to reach out to individuals, changing what they think and not merely what they do, as has been recognized in the outcome document of the Durban Review Conference, which also affirmed the role that the right to freedom of opinion and expression can play in the fight against racism, racial discrimination, xenophobia and related intolerance worldwide."[18]

- "[…] laws to combat hate speech must be carefully construed and applied by the judiciary not to excessively curtail legitimate types of expression. At the same time, while laws are certainly necessary and an important component in addressing hate speech, they should be complemented by a broad set of policy measures to bring about genuine changes in mindsets, perception and discourse. Such a multilayered approach, supported by political and social will and commitment to effecting change, not only aids in addressing less severe forms of hate speech, but also supports awareness-raising and prevention."[19]

- "With regard to the dissemination of hate speech online, States should request the removal of content only through a court order and intermediaries should never be held liable for

[17] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, Report of the Special Rapporteur to the Human Rights Council on the protection of journalists and media freedom, UN Doc. A/HRC/20/17, 4 June 2012, para. 96.
[18] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Report of the Special Rapporteur to the General Assembly on the right to freedom of opinion and expression exercised through the Internet, *UN Doc. A/66/290*, 10 August 201, para. 41.
[19] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Report of the Special Rapporteur to the General Assembly on hate speech and incitement to hatred, *UN Doc. A/67/357*, 7 September 2012, para. 76.

content of which they are not the authors. The right of individuals to express themselves anonymously online must also be fully guaranteed."[20]

C. Questions related to the field of Privacy

- **Question (12)**: *What principles should ensure respect for the right to privacy?*

- "Interference with an individual's right to privacy is only permissible under international human rights law if it is neither arbitrary nor unlawful. In its general comment No. 16, the Human Rights Committee explained that the term "unlawful" implied that no interference could take place "except in cases envisaged by the law. Interference authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant". "The expression "arbitrary interference" can also extend to interference provided for under the law. The introduction of this concept, the Committee explained, "is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances". The Committee interpreted the concept of reasonableness to indicate that "any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case"."[21]

- "These authoritative sources point to the overarching principles of legality, necessity and proportionality, the importance of which also was highlighted in many of the contributions received. To begin with, any limitation to privacy rights reflected in article 17 must be provided for by law, and the law must be sufficiently accessible, clear and precise so that an individual may look to the law and ascertain who is authorized to conduct data surveillance and under what circumstances. The limitation must be necessary for reaching a legitimate aim, as well as in proportion to the aim and the least intrusive option available. Moreover, the limitation placed on the right (an interference with privacy, for example, for the purposes of protecting national security or the right to life of others) must be shown to have some chance of achieving that goal. The onus is on the authorities seeking to limit the right to show that the limitation is connected to a legitimate aim. Furthermore, any limitation to the right to privacy must not render the essence of the right meaningless and must be consistent with other human rights, including the prohibition of discrimination.

[20] Report of the Special Rapporteur to the General Assembly on hate speech and incitement to hatred, *supra*, para. 87.
[21] The right to privacy in the digital age, *supra*, para. 21.

Where the limitation does not meet these criteria, the limitation would be unlawful and/or the interference with the right to privacy would be arbitrary."[22]

- "[…] the Human Rights Committee has underscored the importance of "measures to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity regardless of the nationality or location of individuals whose communications are under direct surveillance"."[23]

- "States' obligations under article 17 of the International Covenant on Civil and Political Rights include the obligation to respect the privacy and security of digital communications. This implies in principle that individuals have the right to share information and ideas with one another without interference by the State, secure in the knowledge that their communication will reach and be read by the intended recipients alone. Measures that interfere with this right must by authorized by domestic law that is accessible and precise and that conforms with the requirements of the Covenant. They must also pursue a legitimate aim and meet the tests of necessity and proportionality."[24]

- "International human rights law requires States to provide an articulable and evidence-based justification for any interference with the right to privacy, whether on an individual or mass scale. It is a central axiom of proportionality that the greater the interference with protected human rights, the more compelling the justification must be if it is to meet the requirements of the Covenant. The hard truth is that the use of mass surveillance technology effectively does away with the right to privacy of communications on the Internet altogether. By permitting bulk access to all digital communications traffic, this technology eradicates the possibility of any individualized proportionality analysis. It permits intrusion on private communications without independent (or any) prior authorization based on suspicion directed at a particular individual or organization. Ex ante scrutiny is therefore possible only at the highest level generality. Since there is no target-specific justification for measures of mass surveillance, it is incumbent upon relevant States to justify the general practice of seeking bulk access to digital communications. The proportionality analysis thus shifts from the micro level (assessing the justification for invading a particular individual's or organization's privacy) to the macro level (assessing the justification for adopting a system that involves wholesale interference with the individual and collective privacy rights of all Internet users). The sheer scale of the interference with privacy rights calls for a competing public policy justification of

[22] The right to privacy in the digital age, *supra*, para. 23.
[23] The right to privacy in the digital age, *supra*, para. 36.
[24] Report of the Special Rapporteur to the General Assembly on the promotion and protection of human rights and fundamental freedoms while countering terrorism, *UN Doc. A/69/397*, 23 September 2014, para. 58.

analogical magnitude. As an absolute minimum, article 17 requires States using mass surveillance technology to give a meaningful public account of the tangible benefits that accrue from its use. Without such a justification, there is simply no means to measure the compatibility of this emerging State practice with the requirements of the Covenant. An assessment of proportionality in this context involves striking a balance between the societal interest in the protection of online privacy, on the one hand, and the undoubted imperatives of effective counter-terrorism and law enforcement, on the other."[25]

- **Question (14)**: *What is the importance of transparency around limitations of privacy?*

- "Paragraph 2 of article 17 of the International Covenant on Civil and Political Rights explicitly states that everyone has the right to the protection of the law against unlawful or arbitrary interference with their privacy. This implies that any communications surveillance programme must be conducted on the basis of a publicly accessible law, which in turn must comply with the State's own constitutional regime and international human rights law. "Accessibility" requires not only that the law is published, but that it is sufficiently precise to enable the affected person to regulate his or her conduct, with foresight of the consequences that a given action may entail. The State must ensure that any interference with the right to privacy, family, home or correspondence is authorized by laws that (a) are publicly accessible; (b) contain provisions that ensure that collection of, access to and use of communications data are tailored to specific legitimate aims; (c) are sufficiently precise, specifying in detail the precise circumstances in which any such interference may be permitted, the procedures for authorizing, the categories of persons who may be placed under surveillance, the limits on the duration of surveillance, and procedures for the use and storage of the data collected; and (d) provide for effective safeguards against abuse. Consequently, secret rules and secret interpretations – even secret judicial interpretations – of law do not have the necessary qualities of "law". Neither do laws or rules that give the executive authorities, such as security and intelligence services, excessive discretion; the scope and manner of exercise of authoritative discretion granted must be indicated (in the law itself, or in binding, published guidelines) with reasonable clarity. A law that is accessible, but that does not have foreseeable effects, will not be adequate. The secret nature of specific surveillance powers brings with it a greater risk of arbitrary exercise of discretion which, in turn, demands

[25] Report of the Special Rapporteur to the General Assembly on the promotion and protection of human rights and fundamental freedoms while countering terrorism, *supra*, paras. 12, 13,14.

greater precision in the rule governing the exercise of discretion, and additional oversight."[26]

- "States should be completely transparent about the use and scope of communications surveillance techniques and powers. They should publish, at minimum, aggregate information on the number of requests approved and rejected, a disaggregation of the requests by service provider and by investigation and purpose. States should provide individuals with sufficient information to enable them to fully comprehend the scope, nature and application of the laws permitting communications surveillance. States should enable service providers to publish the procedures they apply when dealing with State communications surveillance, adhere to those procedures, and publish records of State communications surveillance. States should establish independent oversight mechanisms capable to ensure transparency and accountability of State surveillance of communications."[27]

- "It is a prerequisite for any assessment of the lawfulness of these measures that the States using the technology be transparent about their methodology and its justification. Otherwise, there is a risk that systematic interference with the security of digital communications will continue to proliferate without any serious consideration being given to the implications of the wholesale abandonment of the right to online privacy. If States deploying this technology retain a monopoly of information about its impact, a form of conceptual censorship will prevail that precludes informed debate." "The very purpose of the Covenant's requirement for explicit and publicly accessible legislation governing State interference with communications is to enable individuals to know the extent of the privacy rights they actually enjoy and to foresee the circumstances in which their communications may be subjected to surveillance."[28]

- "Accessibility requires not only that domestic law be published, but also that it meet a standard of clarity and precision sufficient to enable those affected to regulate their conduct with foresight of the circumstances in which intrusive surveillance may occur. In paragraph 8 of its general comment No. 16 on the right to privacy, the Human Rights Committee stressed that legislation authorizing interference with private communications "must specify in detail the precise circumstances in which such interference may be permitted"."

[26] The right to privacy in the digital age, *supra*, paras. 28, 29.
[27] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, Report of the Special Rapporteur to the Human Rights Council on the implications of States' surveillance of communications on the exercise of the human rights to privacy and to freedom of opinion and expression, *UN Doc. A/HRC/23/40*, 17 April 2013, paras. 91, 92, 93.
[28] Report of the Special Rapporteur to the General Assembly on the promotion and protection of human rights and fundamental freedoms while countering terrorism, *supra*, paras. 14, 15.

"[…] this stipulation had always been understood as requiring domestic legislation to spell out clearly the conditions under which, and the procedures by which, any interference may be authorized; the categories of person whose communications may be intercepted; the limits on the duration of surveillance; and the procedures for the use and storage of the data collected. The European Court of Human Rights has also stressed the need for clear detailed rules on the subject."[29]

- **Question (15)**: *What kinds of arrangements can help to safeguard the exercise of privacy in relation to other rights?*

- "Article 17, paragraph 2 of the International Covenant on Civil and Political Rights states that everyone has the right to the protection of the law against unlawful or arbitrary interference or attacks. The "protection of the law" must be given life through effective procedural safeguards, including effective, adequately resourced institutional arrangements. It is clear, however, that a lack of effective oversight has contributed to a lack of accountability for arbitrary or unlawful intrusions on the right to privacy in the digital environment. Internal safeguards without independent, external monitoring in particular have proven ineffective against unlawful or arbitrary surveillance methods. While these safeguards may take a variety of forms, the involvement of all branches of government in the oversight of surveillance programmes, as well as of an independent civilian oversight agency, is essential to ensure the effective protection of the law."[30]

- "Judicial involvement that meets international standards relating to independence, impartiality and transparency can help to make it more likely that the overall statutory regime will meet the minimum standards that international human rights law requires." "Attention is therefore turning increasingly towards mixed models of administrative, judicial and parliamentary oversight." "There is particular interest in the creation of "public interest advocacy" positions within surveillance authorization processes." "The utility of independent advice, monitoring and/or review to help to ensure strict scrutiny of measures imposed under a statutory surveillance regime has been highlighted positively in relevant jurisprudence." "Jurisprudence at the regional level has emphasized the utility of an entirely independent oversight body, particularly to monitor the execution of approved surveillance measures. In 2009, the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism suggested, therefore,

[29] Report of the Special Rapporteur to the General Assembly on the promotion and protection of human rights and fundamental freedoms while countering terrorism, *supra*, para. 36.
[30] The right to privacy in the digital age, *supra*, para. 37.

that "there must be no secret surveillance system that is not under review of an independent oversight body and all interferences must be authorized through an independent body"."[31]

- "The Special Rapporteur concurs with the High Commissioner for Human Rights that there is an urgent need for States using this technology to revise and update national legislation to ensure consistency with international human rights law. Not only is this a requirement of article 17, but it also provides an important opportunity for informed debate that can raise public awareness and enable individuals to make informed choices. Where the privacy rights of the entire digital community are at stake, nothing short of detailed and explicit primary legislation should suffice. Appropriate restrictions should be imposed on the use that can be made of captured data, requiring relevant public authorities to provide a legal basis for the reuse of personal information. States should establish strong and independent oversight bodies that are adequately resourced and mandated to conduct ex ante review, considering applications for authorization not only against the requirements of domestic law, but also against the necessity and proportionality requirements of the Covenant. In addition, individuals should have the right to seek an effective remedy for any alleged violation of their online privacy rights. This requires a means by which affected individuals can submit a complaint to an independent mechanism that is capable of conducting a thorough and impartial review, with access to all relevant material and attended by adequate due process guarantees. Accountability mechanisms can take a variety of forms, but must have the power to order a binding remedy. States should not impose standing requirements that undermine the right to an effective remedy."[32]

- "The Special Rapporteur considers that there is an urgent need for States to revise national laws regulating modern forms of surveillance to ensure that these practices are consistent with international human rights law. Domestic laws governing the interception of communications should be updated to reflect modern forms of digital surveillance that are far broader in scope, and involve far deeper penetration into the private sphere, than those envisaged when much the existing domestic legislation was enacted. The absence of clear and up-to-date legislation creates an environment in which arbitrary interferences with the right to privacy can occur without commensurate safeguards. Explicit and detailed laws are essential for ensuring legality and proportionality in this context. They are also an indispensable means of enabling individuals to foresee whether and in what circumstances their communications may be the subject of surveillance. A public legislative process provides an opportunity for Governments to justify mass surveillance measures to the

[31] The right to privacy in the digital age, *supra*, para. 38.
[32] Report of the Special Rapporteur to the General Assembly on the promotion and protection of human rights and fundamental freedoms while countering terrorism, *supra*, paras. 59, 60, 61.

public. Open debate enables the public to appreciate the balance that is being struck between privacy and security. A transparent law-making process should also identify the vulnerabilities inherent in digital communications systems, enabling users to make informed choices."[33]

- "One of the core protections afforded by article 17 is that covert surveillance systems must be attended by adequate procedural safeguards to protect against abuse. These safeguards may take a variety of forms, but generally include independent prior authorization and/or subsequent independent review. Best practice requires the involvement of the executive, the legislature and the judiciary, as well as independent civilian oversight (see A/HRC/27/37). The absence of adequate safeguards can lead to a lack of accountability for arbitrary or unlawful intrusions on the right to Internet privacy." "The other procedural dimension of article 17 is the requirement for ex post facto review of intrusive surveillance measures. Some States provide for an independent reviewer to monitor the operation of surveillance legislation by analysing the manner and extent of its use and the justification therefor. Such reviews should always incorporate an analysis of the compatibility of State practice with the requirements of the Covenant."[34]

- **Question (17)**: *What may be the impact of issues relating to big data on respect for privacy?*

- "It has been suggested by some that the conveyance and exchange of personal information via electronic means is part of a conscious compromise through which individuals voluntarily surrender information about themselves and their relationships in return for digital access to goods, services and information. Serious questions arise, however, about the extent to which consumers are truly aware of what data they are sharing, how and with whom, and to what use they will be put. According to one report, "a reality of big data is that once data is collected, it can be very difficult to keep anonymous. While there are promising research efforts underway to obscure personally identifiable information within large data sets, far more advanced efforts are presently in use to re-identify seemingly 'anonymous' data. Collective investment in the capability to fuse data is many times greater than investment in technologies that will enhance privacy." Furthermore, the authors of the report noted that "focusing on controlling the collection and retention of

[33] Report of the Special Rapporteur to the General Assembly on the promotion and protection of human rights and fundamental freedoms while countering terrorism, *supra*, paras. 38, 39.
[34] Report of the Special Rapporteur to the General Assembly on the promotion and protection of human rights and fundamental freedoms while countering terrorism, *supra*, paras. 45, 48.

personal data, while important, may no longer be sufficient to protect personal privacy", in part because "big data enables new, non-obvious, unexpectedly powerful uses of data"."[35]

- "One factor that must be considered in determining proportionality is what is done with bulk data and who may have access to them once collected. Many national frameworks lack "use limitations", instead allowing the collection of data for one legitimate aim, but subsequent use for others. The absence of effective use limitations has been exacerbated since 11 September 2001, with the line between criminal justice and protection of national security blurring significantly. The resulting sharing of data between law enforcement agencies, intelligence bodies and other State organs risks violating article 17 of the Covenant, because surveillance measures that may be necessary and proportionate for one legitimate aim may not be so for the purposes of another. A review of national practice in government access to third-party data found "when combined with the greater ease with which national security and law enforcement gain access to private-sector data in the first place, the expanding freedom to share that information among agencies and use it for purposes beyond those for which it was collected represents a substantial weakening of traditional data protections"."[36]

E. Broader issues

- **Question (24)**: *What international, regional and national frameworks, normative guidelines and accountability mechanisms exist of relevance to one or more fields of the study?*

- "As recalled by the General Assembly in its resolution 68/167, international human rights law provides the universal framework against which any interference in individual privacy rights must be assessed. Article 12 of the Universal Declaration of Human Rights provides that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." The International Covenant on Civil and Political Rights, to date ratified by 167 States, provides in article 17 that "no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation". It further states that "everyone has the right to the protection of the law against such interference or attacks." Other international human rights instruments contain similar

[35] The right to privacy in the digital age, *supra*, para. 18.
[36] The right to privacy in the digital age, *supra*, para. 27.

provisions. Laws at the regional and national levels also reflect the right of all people to respect for their private and family life, home and correspondence or the right to recognition and respect for their dignity, personal integrity or reputation. In other words, there is universal recognition of the fundamental importance, and enduring relevance, of the right to privacy and of the need to ensure that it is safeguarded, in law and in practice."[37]

- "In its general comment No. 16, the Human Rights Committee underlined that compliance with article 17 of the International Covenant on Civil and Political Rights required that the integrity and confidentiality of correspondence should be guaranteed de jure and de facto."[38]

- "The Guiding Principles on Business and Human Rights, endorsed by the Human Rights Council in 2011, provide a global standard for preventing and addressing adverse effects on human rights linked to business activity. The responsibility to respect human rights applies throughout a company's global operations regardless of where its users are located, and exists independently of whether the State meets its own human rights obligations."[39]

- "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."[40]

- **Question (25)**: *How do cross-jurisdictional issues operate with regard to freedom of expression and privacy?*

- "[…]digital surveillance therefore may engage a State's human rights obligations if that surveillance involves the State's exercise of power or effective control in relation to digital communications infrastructure, wherever found, for example, through direct tapping or

[37] The right to privacy in the digital age, *supra*, paras. 12,13.
[38] The right to privacy in the digital age, *supra*, para. 17.
[39] The right to privacy in the digital age, *supra*, para. 43.
[40] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, Report of the Special Rapporteur to the Human Rights Council on key trends and challenges to the right of all individuals to seek, receive and impart information and ideas of all kinds through the Internet, *UN Doc. A/HRC/17/27*, 16 May 2011, para. 21.

penetration of that infrastructure. Equally, where the State exercises regulatory jurisdiction over a third party that physically controls the data, that State also would have obligations under the Covenant. If a country seeks to assert jurisdiction over the data of private companies as a result of the incorporation of those companies in that country, then human rights protections must be extended to those whose privacy is being interfered with, whether in the country of incorporation or beyond."[41]

- "The Special Rapporteur concurs with the High Commissioner for Human Rights that where States penetrate infrastructure located outside their territorial jurisdiction, they remain bound by their obligations under the Covenant. Moreover, article 26 of the Covenant prohibits discrimination on grounds of, inter alia, nationality and citizenship. The Special Rapporteur thus considers that States are legally obliged to afford the same privacy protection for nationals and non-nationals and for those within and outside their jurisdiction. Asymmetrical privacy protection regimes are a clear violation of the requirements of the Covenant."[42]

- **Question (26)**: *What are the intersections between the fields of study: for example, between access and freedom of expression; privacy and freedom of expression?*

- "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."[43]

- "States cannot ensure that individuals are able to freely seek and receive information or express themselves without respecting, protecting and promoting their right to privacy. Privacy and freedom of expression are interlinked and mutually dependent; an

[41] The right to privacy in the digital age, *supra*, para. 34.
[42] Report of the Special Rapporteur to the General Assembly on the promotion and protection of human rights and fundamental freedoms while countering terrorism, *supra*, para. 62.
[43] Report of the Special Rapporteur to the Human Rights Council on key trends and challenges to the right of all individuals to seek, receive and impart information and ideas of all kinds through the Internet, *supra*, para. 53.

infringement upon one can be both the cause and consequence of an infringement upon the other. Without adequate legislation and legal standards to ensure the privacy, security and anonymity of communications, journalists, human rights defenders and whistleblowers, for example, cannot be assured that their communications will not be subject to States' scrutiny."[44]

- "…other rights also may be affected by mass surveillance, the interception of digital communications and the collection of personal data. These include the rights to freedom of opinion and expression, and to seek, receive and impart information; to freedom of peaceful assembly and association; and to family life – rights all linked closely with the right to privacy and, increasingly, exercised through digital media. Other rights, such as the right to health, may also be affected by digital surveillance practices, for example where an individual refrains from seeking or communicating sensitive health-related information for fear that his or her anonymity may be compromised. There are credible indications to suggest that digital technologies have been used to gather information that has then led to torture and other ill-treatment."[45]

- "…, the Special Rapporteur would like to reiterate that States have a positive obligation to promote or to facilitate the enjoyment of the right to freedom of expression and the means necessary to exercise this right, which includes the Internet. Moreover, access to the Internet is not only essential to enjoy the right to freedom of expression, but also other rights, such as the right to education, the right to freedom of association and assembly, the right to full participation in social, cultural and political life and the right to social and economic development."[46]

REFERENCE DOCUMENTS

- The right to privacy in the digital age - Report of the Office of the United Nations High Commissioner for Human Rights, *UN Doc. A/HRC/27/37*, 30 June 2014.

- Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, *UN Doc. A/69/397*, 23 September 2014.

[44] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, Report of the Special Rapporteur to the Human Rights Council on the implications of States' surveillance of communications on the exercise of the human rights to privacy and to freedom of opinion and expression, *UN Doc. A/HRC/23/40*, 17 April 2013, para. 79.
[45] The right to privacy in the digital age, supra, para. 14.
[46] Report of the Special Rapporteur to the General Assembly on the right to freedom of opinion and expression exercised through the Internet, *supra*, para. 61.

- Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, on the implications of States' surveillance of communications on the exercise of the human rights to privacy and to freedom of opinion and expression, *UN Doc. A/HRC/23/40*, 17 April 2013.

- Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, on hate speech and incitement to hatred, *UN Doc. A/67/357*, 7 September 2012.

- Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, Report of the Special Rapporteur on the protection of journalists and media freedom, *UN Doc. A/HRC/20/17*, 4 June 2012.

- Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, on the right to freedom of opinion and expression exercised through the Internet, *UN Doc. A/66/290*, 10 August 2011.

- Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, on key trends and challenges to the right of all individuals to seek, receive and impart information and ideas of all kinds through the Internet, *UN Doc. A/HRC/17/27*, 16 May 2011.

- Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Tenth anniversary joint declaration: Ten key challenges to freedom of expression in the next decade, *UN Doc. A/HRC/14/23/Add.2*, 25 March 2010.

November 2014