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

1. What can be done to reinforce the right to seek and receive information in the online environment?

The right to seek and receive information in the online environment can be reinforced by encouraging the implementation of Recommendations of particular relevance, adopted by the Committee of Ministers, on the public service value of the Internet (CM/Rec(2007)16 of 7 November 2007) and on the Guide to human rights for Internet users (CM/Rec(2014)6 of 16 April 2014). These standards recommend government-led multi-stakeholder efforts to promote access: (i) individuals should not be disconnected from the Internet against their will, except when it is decided by a court. In certain cases, contractual arrangements may also lead to discontinuation of service but this should be a measure of last resort; (ii) Access should be affordable and non-discriminatory. There should be the greatest possible access to Internet content, applications and services using the devices of an individuals' choice; (iii) Public authorities should make reasonable efforts and to take specific measures to facilitate access to the Internet also when individuals live in rural and geographically remote areas, those on low income, disadvantaged groups such as the elderly, and/or those special needs or disabilities; (iv) Access also means that there should be no discrimination with public authorities, Internet service providers and providers of online content and services, or with other users or groups of users, in particular on any grounds such as gender, race, colour, language, religion or belief, political or other opinion, national or social origin, association with a national minority, property, birth or other status, including ethnicity, age or sexual orientation. Promoting access to/ participation in culture and the cultural implications of digitisation is another means of reinforcing the right. This is being carried out via a Council of Europe platform for the exchange of experiences and good practices for policy makers, practitioners and civil society.

Addressing interferences with people's access to information on the Internet, such as through blocking and filtering measures, is another way of reinforcing the right. Measures consisting in the wholesale blocking of online content can produce arbitrary and collateral effects because they render large amounts of information inaccessible for Internet users. Moreover, disconnecting people from the Internet and blocking access to entire web platforms or sites must be evaluated and applied with utmost circumspection having regard to the criteria established by the European Court of Human Rights (the Court) under Article 10 of the European Convention on Human Rights (the ECHR) in relation to their necessity in a democratic society, notably the existence of a pressing social need and the principle of proportionality. In Ahmet Yıldırım v. Turkey (no. 3111/10), the Court held, on 18 December 2012, that there had been a violation of Article 10 (freedom of expression) of the Convention. It found that the effects of a court decision which led to the blanket blocking of access to Google sites had been arbitrary and the judicial review of the blocking of access had been insufficient to prevent abuses.

2. What mechanisms can develop policies and common standards for open-licensed educational resources and scientific repositories, and for the long-term preservation of digital heritage?

The Council of Europe provides a mechanism for the development of policies and standards as well as capacity building. Pursuant to the Recommendation, adopted by the Committee of

Ministers, on the public service value of the Internet (CM/Rec(2007)16 of 7 November 2007), member states are encouraged to: (i) develop strategies and policies and create appropriate legal and institutional frameworks to preserve the digital heritage of lasting cultural, scientific, or other values, in co-operation with holders of copyright and neighbouring rights, and other legitimate stakeholders in order, where appropriate, to set common standards and ensure compatibility and share resources. In this regard, access to legally deposited digital heritage materials, within reasonable restrictions, should also be assured; (ii) develop a culture of participation and involvement, inter alia by providing for the creation, modification and remixing of interactive content and the transformation of consumers into active communicators and creators of content; (iii) promote mechanisms for the production and distribution of user- and community-generated content (thereby facilitating online communities), inter alia by encouraging public service media to use such content and co-operate with such communities; (iv) encourage the creation and processing of and access to educational, cultural and scientific content in digital form, so as to ensure that all cultures can express themselves and have access to the Internet in all languages, including indigenous ones.

3. How can greater progress be made as regards inclusive strategies for women and girls as well as marginalized and disabled people?

Gender equality means equal visibility, empowerment, responsibility and participation of both women and men in all spheres of public life, including the media. Pursuant to the Recommendation, adopted by the Committee of Ministers, on gender equality and the media (CM/Rec(2013)1 of 10 July 2013) member states are encouraged to: (i) adopt legal frameworks to ensure respect for the principle of human dignity and the prohibition of all discrimination; (ii) ensure that media regulators respect gender equality principles in their decision making and practice; (iii) support awareness-raising initiatives and campaigns on combating gender stereotypes in the media. Further, media organisations are encouraged to adopt self-regulatory measures, internal codes of conduct/ethics and internal supervision, and develop standards in media coverage that promotes gender equality, in order to promote a consistent internal policy and working conditions aimed at: (i) equal access to, and representation in, media work for women and men, including in the areas where women are underrepresented; (ii) a balanced participation of women and men in management posts, in bodies with an advisory, regulatory or internal supervisory role, and generally in the decision-making process; (iii) a non-stereotyped image, role and visibility of women and men, avoidance of sexist advertising, language and content which could lead to discrimination on grounds of sex, incitement to hatred and gender-based violence. All of the above should be facilitated by means of a review and update of the legal framework on media, and by means of mandating media regulators and requiring public service media to assess the implementation of gender equality policy.

In general terms, gender mainstreaming should be automatically factored into all new strategies, educational programmes, etc., with a view to achieving substantive equality. Preliminary research in this area should be carried out on the basis of sex, disability, etc. disaggregated figures to ensure a representative picture of the requirements is built, before drawing up strategies and educational programmes.

4.How can accessibility be facilitated through increases in locally produced and relevant content in different languages?

Pursuant to the Recommendation, adopted by the Committee of Ministers, on the public service value of the Internet (CM/Rec(2007)16 of 7 November 2007), member states are encouraged to

ensure that all cultures can express themselves and have access to the Internet in all languages, including indigenous ones. This includes promoting access to a multilingual Internet, capacity building for the production of local and indigenous content on the Internet. The Recommendation also encourages access to educational, cultural and scientific content in digital form, developing a culture of participation (for example by providing for the creation, modification and remixing of interactive content), and the promotion of user- and community-generated content.

5.What can be done to institutionalize MIL effectively in national educational systems?

Agreement needs to be reached on a clear definition of MIL to promote institutionalisation. On this basis, an educational framework could be drawn up by governments for educational and cultural institutions. In this connection, there could be recognition of the new professions arising from digitization, and the institution of an appropriate educational programme to support these new professions. This could be complemented by: (i) the collection (compilation) of concepts, action plans, guidelines, practices and resources for the development of MIL in *all* educational/cultural settings in member states (informal, non-formal and formal learning settings), as well as the development of a new thematic space for example within the Council of Europe Compendium on cultural policies (www.culturalpolicies.net) to accommodate relevant information on media literacy policies and link this to external sources (i.e. the *translit* database - www.translit.fr - that holds 29 country profiles on media education); (ii) an awareness-raising campaign for MIL development; (iii) training courses on the development of MIL in different educational and cultural settings; (iv) a MIL campaign to empower citizens; (v) synergies and partnerships between international and European organisations such as Council of Europe, UNESCO, and the European Union.

B. Questions related to the field of Freedom of Expression

6. What are the current and emerging challenges relevant to freedom of expression online?

In his 2014 report on the State of Democracy, Human Rights and the Rule of Law in Europe, the Secretary General placed the rights to freedom of expression and to information at the top of his exposé of political freedoms and democracy, alongside association and assembly. He said "Exercised collectively, these freedoms form the checks and balances necessary to a democratic society." He signalled serious problems in the CoE 47 member states, which include:

- recurring threats to the freedom of expression,
- overzealous recourse to defamation laws,
- violence against journalists,
- impunity in cases of violence against journalists which eases the way for more attacks,
- legislation and practices which limit Internet freedom, mass surveillance.

Anything that can silence, gag or chill media and journalists is a challenge. Journalists and media organisations operate in an increasingly unsafe environment online. They have been the

targets of digital surveillance and hacking attacks, which affects their privacy and the right not to disclose their sources of information.

Reconciling freedom of expression and the protection of the reputation of others is also a challenge. Internet platforms and services which facilitate the sharing of content produced or uploaded by users, faced with strict liability regimes for defamation or other harmful content, such as hate speech, can become bottle-necks for the free flow of information online. The responsibilities for moderating online comments and the extent to which Internet intermediaries have freedom are part of the new notion of media pursuant to the Recommendation adopted by the Committee of Ministers in 2011 (CM/Rec(2011)7 of 21 September 2011). This issue is now being addressed by the European Court of Human Rights in the case of Delfi v. Estonia (no. 64569/09, pending decision of the Grand Chamber).

Interferences with people's access to information on the Internet through blocking and filtering measures are a major concern. In some cases, national legislation that provides the legal basis for these measures lends itself to misuse because it is too broad, lacks clarity and foreseeability with regard to its implementation, confers discretionary powers to the executive and lacks safeguards regarding judicial or independent review. The responses to these challenges should not be at the expense of freedom of expression. Quite the opposite, defending and promoting freedom of expression on the Internet can contribute to creating an environment, both in the physical world and online, where communities reject and counter hatred and intolerance by resorting to free speech which promotes respect for human rights, rule of law, cultural diversity, dialogue and mutual understanding.

Challenges to online freedom of expression can also be seen in the distributed denial-of-service attacks against websites of independent media, human rights defenders, dissidents, whistle-blowers and other new media actors. This has been recognised in the Declaration, adopted on 7 December 2011 by the Committee of Ministers, on freedom of expression and freedom of assembly and association with regard to privately operated Internet platforms and online service providers. These attacks represent an interference with freedom of expression and the right to impart and receive information and, in certain cases, with the right to freedom of association. Companies that provide web hosting services lack the incentive to continue hosting those websites if they fear that the latter will come under attack or if their content may be regarded as sensitive. These companies are not immune to undue interference; their decisions sometimes stem from direct political pressure or from politically motivated economic compulsion, invoking justification on the basis of compliance with their terms of service.

Disconnecting people from the Internet and blocking access to entire web platforms or sites can also be a challenge and should be evaluated and applied with utmost circumspection having regard to the criteria established by the Court under Article 10 of the ECHR in relation to their necessity in a democratic society, notably the existence of a pressing social need and the principle of proportionality. Measures consisting in the wholesale blocking of online content can produce arbitrary and collateral effects because they render large amounts of information inaccessible for Internet users.

Anything which challenges users access to Internet-based content, applications and services of their choice, whether or not they are offered free of charge, using suitable devices of their choice, could interfere with freedom of expression and access to information online.

7. How can legislation in a diverse range of fields which impact on the Internet respect freedom of expression in line with international standards?

Legislation governing privacy and national security can impact on freedom of expression. Unlawful and arbitrary interferences with individuals' privacy on the Internet have a negative impact on the enjoyment of freedom of expression. The fear of having communications or activities online monitored can lead to self-censorship and can have a chilling effect. The interception of online data for reasons of national security has shaken trust in the protection of personal data and privacy online, as stated in the Declaration adopted on 11 June 2013 by the Committee of Ministers on tracking and surveillance. The protection of national security constitutes a public interest imperative yet, in the absence of effective guarantees against misuse or abuse, the measures taken can have far-reaching consequences for the enjoyment of freedom of expression online.

Legislation and practice (e.g. guidelines on prosecuting cases involving communications sent via social media) can be positively used to demonstrate vigilance and commitment by governments to the protection of freedom of expression on the Internet. Legislation which reaffirms that any interference with freedom of expression must meet the tests of legality, necessity and proportionality as enshrined in Article 10, paragraph 2 of the ECHR, provides an important guarantee by the state to its citizens that can be, in turn, reinforced by national courts.

Considering the myriad of fields and their impact on freedom of expression, it would be important to ensure that there are human rights assessments ('human rights proofing') of legislative initiatives and processes as far as possible.

8. Is there a need for specific protections for freedom of expression for the Internet?

Freedom of expression is rapidly evolving and being challenged because of the Internet. It is constantly under review in the framework of the Council of Europe's standard-setting activities.

Narrowly circumscribing limitations to freedom of expression is a way of reducing the margin of appreciation of member states to interfere with this right. The European Court of Human Rights does exactly this by applying a three-step test to assess whether any interference can be justified in compliance with Article 10 para 2 of the ECHR.

Freedom of expression on the Internet could be further protected by committing to do no harm to the universality, integrity and openness of the Internet. Efforts to protect Internet freedom beyond free speech could help recognize the need for a cautious approach by national government efforts to protect their citizens by regulating the Internet.

9. To what extent do laws protect digitally interfaced journalism and journalistic sources?

Anything that can silence, gag or chill media and journalists is a challenge. Journalists and media organisations operate in an increasingly unsafe environment online. The States' duty to create an enabling environment for a safe and free journalism applies offline as well as online.

As stated in Resolution No.2 of the Council of Europe conference of ministers responsible for media and information society (Belgrade, 7-8 November 2013), the Council of Europe recognises that the protection of journalistic sources as a condition for investigative journalism remains of critical importance in the digital age, considering the necessity for media to ascertain the authenticity of content received from multiple sources without exposing them to tracking and reprisal. This can be achieved by creating a favourable legal environment for investigative journalism and critical scrutiny of all matters of public interest. Media regulation, including co-regulation or regulated self-regulation, should comply with the requirements of Article 10 of the ECHR.

In the framework of its cooperation activities, the Council of Europe is helping to raise awareness and empower journalists and other media actors in order to protect themselves online. On 30 April 2014, The Committee of Ministers adopted a Declaration on the protection of journalism and safety of journalists and other media actors. This is currently being followed up and further developed with guidelines as part of a Recommendation elaborated by an expert committee to be adopted by the Committee of Ministers. There is also on-going work on the development of a web-based platform on the protection of journalism and safety of journalists. On 19 December, the Committee of Ministers decided to approve the text of the Memorandum of Understanding between the Council of Europe and partner organisations on the setting-up of this platform, followed by a formal signature event on 4 December 2014.

10. What are the optimum ways to deal with online hate speech? How can Media and Information Literacy empower users to understand and exercise freedom of expression on the Internet?

There are divergent but related approaches being used to combat hate speech: firstly, by prohibition and punishment of “hate speech”, which implies the establishment of legal remedies; and secondly, by providing more media freedom to counter “hate speech” by facilitating the expression for everyone, especially for minorities, and the facilitation of spreading strong and convincing messages of tolerance. Council of Europe member states have adopted standards and strategies to counter hate speech which reflect both approaches.

The Council of Europe No Hate Speech movement aims to combat racism and discrimination and hate speech in online expression by equipping young people and youth organisations with the competences necessary to recognise and act against such human rights violations. Media and information literacy by means of inter alia surveys, inventory of legal documents, training of bloggers and human rights activists, campaigns and awareness-raising events have all helped to build and empower a network of young people online. To effectively combat hate speech in the digital era, it is essential to bring together all stakeholders involved.

There are several ways to tackle hate speech. For example, the Council of Europe Committee of Ministers Recommendation on a new notion of media (CM/Rec(2011)7 of 21 September 2011) provides criteria and indicators for identifying media and guidance on responsibilities, including as regards hate speech. From this Recommendation, the message is clear: media, including new forms of mass communication “should refrain from conveying hate speech and other content that incites violence or discrimination for whatever reason. Special attention is

needed on the part of actors operating collective online shared spaces which are designed to facilitate interactive mass communication (…). They should be attentive to the use of, and editorial response to, expressions motivated by racist, xenophobic, anti-Semitic, misogynist, sexist (including as regards LGBT people) or other bias. Actors in the new media ecosystem may be required (by law) to report to the competent authorities criminal threats of violence based on racial, ethnic, religious, gender or other grounds that come to their attention."

11. What are the optimum systems for independent self-regulation by journalistic actors and intermediaries in cyberspace?

Embracing a new notion of media, as stated in the Recommendation of the Committee of Ministers adopted in September 2011 (CM/Rec(2011)7 of 21 September 2011), will help all actors – whether new or traditional – in being guaranteed an appropriate level of protection and in being provided with a clear indication of their duties and responsibilities. This Recommendation recommends to member states inter alia to: (i) review regulatory needs in respect of all actors delivering services or products in the media ecosystem so as to guarantee people's right to seek, receive and impart information in accordance with Article 10 of the European Convention on Human Rights, and to extend to those actors relevant safeguards against interference that might otherwise have an adverse effect on Article 10 rights, including as regards situations which risk leading to undue self-restraint or self-censorship; and (ii) invite traditional and new media to consult each other in order to develop self-regulatory tools, including codes of conduct, which take account of, or incorporate in a suitable form, generally accepted media and journalistic standards.

In this context, Internet intermediaries (e.g. ISPs, and content providers such as Google, Facebook etc.) are part of the new media ecosystem where the production, distribution and consumption of content and information have changed considerably. New questions arise with regard to the balancing exercise that is necessary in defamation cases between the right to freedom of expression on the one hand and the protection of the reputation of others on the other hand. Internet platforms and services which facilitate the sharing of content produced or uploaded by users, when faced with strict liability regimes for defamation or other harmful content, such as hate speech, can become bottle-necks for the free flow of information online. The question of Internet intermediaries' liabilities for defamation is before the Court in the case of Delfi v. Estonia (no. 64569/09, pending decision of the Grand Chamber).

Pursuant to the Committee of Ministers Recommendation on the protection of human rights with regard to search engines (CM/Rec(2012)3 of 4 April 2012), enhancing transparency regarding the way in which access to information is provided and the collection and processing of personal data is carried out are ways to optimize the responsibility of intermediaries. Moreover, member states are encouraged to promote transparent self- and co-regulatory mechanisms for search engines, in particular with regard to the accessibility of content declared illegal by a court or competent authority, as well as of harmful content.

C. Questions related to the field of Privacy

12. What principles should ensure respect for the right to privacy?

The right to respect for private and family life is enshrined in Article 8 of the ECHR. This right is further interpreted by the case-law of the European Court of Human Rights as well as complemented and reinforced by the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108). The notion of "private life" includes "a person's right to their image, for example by means of photographs and video-clips" as well as "a person's identity and personal development, the right to establish and develop relationships with other human beings". An individual's right to privacy is at stake when his or her personal information are processed. The respect for this fundamental human right is ensured by the principles within the Council of Europe's Convention 108.

Principle of lawfulness: To ensure the respect for the right to privacy, the processing of personal data is only considered to be lawful if it is in accordance with the law, pursues a legitimate purpose and is necessary in a democratic society in order to achieve the legitimate purpose. In relation to the protection of the right to privacy in general, this principle focusses on the legal basis of the activity which possibly constitutes a violation of the right to privacy as well as the activities' purpose which has to be legitimate and necessary. By fulfilling these requirements the individual's right to privacy is maintained.

Principle of purpose specification and limitation: Before the start of the processing of the data, domestic law has to be considered to decide whether the purpose of processing has to be explicitly defined. A purpose which is specified and limited according to domestic law helps to avoid violations of the right to privacy.

Data quality principles: The data quality principles should also be considered in regards to the ensuring of the right to privacy in general. Firstly, the data processed has to be relevant. The personal information needs to be "adequate, relevant and not excessive in relation to the purpose for which they are collected and/or further processed". Therefore, the personal data processed has to be necessary and proportionate to the legitimate aim. Secondly, the data processed has to be accurate. Personal information shall not be used without taking steps to ensure with reasonable certainty that the data are accurate and up to date. Also, the data processed has to be stored to a limited degree. It is necessary that the data are deleted as soon as they are no longer needed for the purposes for which they were collected. This can only be overseen if it is provided by law and in accordance with appropriate safeguards for the protection of data subjects.

Principle of fair processing: The data subjects must be informed - at least about the purpose of processing and about the identity and address of the controller - before their data is processed. Unless specifically permitted by law, there must be no secret and covert processing of personal data. This notion of transparency within the field of data protection also includes that the data subjects always have the right to be told by the controller on request if their data are being processed, and if so, which ones.

Principle of accountability: There needs to be an active implementation of measures by controllers to promote and safeguard data protection in their processing activities. The

controllers are to take responsibility on their operations under the data protection law and should be able to demonstrate compliance with data protection provisions to data subjects, to the general public and to supervisory authorities. There are additional safeguards for the data subject which include the principles of openness, access to own data, rectification and remedy.

Principle of data security: The personal data obtained has to be stored in a safe manner by implementing "appropriate security measures … against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination".

Principle of the user's consent: The individual has to consent to the processing of his or her data. This can be done by, for example, "agreeing to the terms and conditions of use of an Internet service". The user's consent has to be "a person's free, specific, informed and explicit (unambiguous) consent to the processing of personal data on the Internet".

13. What is the relationship between privacy, anonymity and encryption?

Privacy is the control an individual has over personal information and personal space. In other words, it is the certain degree of intimacy that the individual wishes that determines the notion of privacy when it comes to the privacy of a specific person. This personal privacy can also contain the sphere of anonymity.

The principle of anonymity, as stated by the Committee of Ministers in its Declaration of 28 May 2003 on freedom of communication on the Internet, is first and foremost to underline that the will of users to remain anonymous should be respected. There are two aspects to this principle. Firstly, users may have a valid reason not to reveal their identity when they have statements published on the Internet. Obliging them to do so could restrict excessively their freedom of expression. It would also deprive society of potentially valuable information and ideas. Secondly, users need protection against unwarranted on-line surveillance by public or private entities. Member States should therefore, for example, allow the use of anonymity tools or software which enables users to protect themselves. This principle has, however, its limitations. Member States should have the possibility of obtaining information about persons responsible for illegal activities within the limits laid down under national law, in particular Article 8 ECHR, and other relevant international treaties such as the Convention on Cybercrime. In the case of K.U. v. Finland (no. 2872/02 of 2 December 2008), underlined the need to provide a framework for reconciling the confidentiality of Internet services with the prevention of disorder or crime and the protection of the rights and freedoms of others, and in particular children and other vulnerable individuals.

Anonymity is related to the concept of identity. In order to make a person not identifiable, personal data, for example, can be anonymised. Data are anonymised if all identifying elements have been eliminated from a set of personal data. No element may be left within the information which could, by exercising reasonable effort, serve to re-identify the person(s) concerned. Where data have been successfully anonymised, they are no longer personal data. If personal data no longer serve their initial purpose, but are to be kept in a personalised form for the purpose of historical, statistical or scientific use, Convention 108 allow this possibility on condition that appropriate safeguards against misuse are applied. The data processed can,

therefore, not be associated with a particular individual and the information is anonym. Consequently, the anonymisation of personal data can be seen to be a part of the individuals' control over personal information and sphere, and therefore a notion of the term "privacy". However, as anonymised data are not personal data anymore and can consequently not be linked to the specific individual anymore, the concept of anonymity is to be seen to be broader than the notion of privacy. Concerning current privacy issues in relation to the internet, the notion of anonymity has become increasingly important.

Encryption is the technical aspect of the topic. By encrypting the identifiers, such as a name, date, sex and address, in personal data, the personal information is 'pseudonymised'. To hide identity personal data with encrypted identifiers are widely used. Consequently, this helps the data controllers to ensure that they deal with the same data subjects without the need for the data subjects' real identities. Encryption is therefore a strong link in the armoury of privacy-enhancing technology. Concerning anonymity within search engines, the Recommendation, adopted by the Committee of Ministers, on the protection of human rights with regard to search engines (CM/Rec(2012)3 of 4 April 2012) refers to a number of measures that providers can take to protect their users' privacy. This includes the protection of personal data against unlawful access by third parties and data breach notification schemes. Measures should also include "end-to-end" encryption of the communication between the user and the search engine provider. Cross-correlation of data originating from different services/platforms belonging to a search engine provider can take place only if unambiguous consent has been granted by the user for that specific service.

14. What is the importance of transparency around limitations of privacy?

If the interference with the data subject's right to respect for private life is in accordance with the law, in pursuance of a legitimate aim and necessary in a democratic society it can be held that the individual's right to privacy is not absolute in these circumstances. This is in particular the case when it comes to the interplay with other human rights and interests of private persons or the public in general. The case-law of the ECtHR shows how the individual's sphere of privacy can be justifiably limited by the state.

Interference with privacy can be necessary within a democratic society, it is to be held that "the notion of necessity implies that the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued". Therefore, derogations are permissible "in the interests of: (a) protecting State security, public safety, (…) monetary interests of the State or the suppression of criminal offences; and (b) protecting the data subject or the rights and freedoms of others" (Convention 108). These limitations have to be communicated to the public so that the individuals are aware of the facts concerning their actions within the sphere of privacy. Transparency is the key to achieve that the individuals understand the right to privacy and its limitations.

Limitations to privacy have to be manifested within provisions of domestic law that fulfil certain requirements. For instance, the domestic legal basis has to be accessible to the persons concerned and foreseeable as to its effects. Here, transparency is of particular importance. Recently there has been a vivid discussion about the transparency of domestic legal bases due

to Edward Snowden's revelations in June 2013 concerning the NSA's mass surveillance programme called PRISM and the government's legal pressure on internet companies like Google, Yahoo and others to provide the governmental intelligence agency with their users' data. Following the revelations, several Internet companies put pressure on the US government to publish the domestic legal frameworks that provide for the NSA's mass surveillance and access to the user data stored at the internet companies' servers. This so-called "Snowden effect" resulted in the publishing of transparency reports by the US authorities. Therefore, transparency can be required to prove the limitation's manifestation within domestic law.

15. What kinds of arrangements can help to safeguard the exercise of privacy in relation to other rights?

In order to ensure that the exercise of privacy is safeguarded in relation to other rights it is of particular importance to develop legal frameworks that take into account the different rights and their interplay. Adequate examples can be given in view of the Recommendation, adopted by the Committee of Ministers, to member States on the protection of human rights with regard to social networking services (CM/Rec(2012)4 of 4 April 2012) as well as the Recommendation, adopted by the Committee of Ministers, to member States on the protection of human rights with regard to search engines (CM/Rec(2012)3 of 4 April 2012). These recommendations show how privacy can be ensured also in relation to other rights.

It is also within the responsibility of the ECtHR to define the relation between the right to privacy and other human rights and fundamental freedoms.

The vast majority of member States have set up data protection authorities. These are the actors that play the most "important role in investigating, intervening, raising awareness or otherwise remedying interferences in the processing of personal data". They also have to make sure that the balance of the right to privacy and other rights is maintained.

16. How can openness and transparency of data be reconciled with privacy?

Openness and transparency are central to the protection of privacy because they are contained within the right to privacy and are considered to be essential in order to protect and promote this fundamental right.

The right to access own data as well as the principle of openness are additional safeguards for a data subject to protect his or her personal data. In order to make authorities responsible for their actions in breach of the individual's privacy, they "should be able to demonstrate compliance with data protection provisions to data subjects, to the general public and to supervisory authorities". Only in this case is it possible to meet the requirement of accountability enshrined in Convention 108. The openness and transparency of data is also an issue being dealt with during the modernisation of Convention 108.

18.How can security of personal data be enhanced?

The T-PD notes that the security of the exchanges and the systems is a vital aspect which requires adequate technical and organisational measures to be adopted so as to ensure both the reliability and integrity of the data and the relevant processing and also the confidentiality thereof. It underlines the importance of meeting the requirements of Article 7 of Convention 108 and ensuring the security of the entire system by laying down strict rules on encryption of data, access to data, identification of the persons to whom the data are transferred and rules on the full traceability of the exchanges, in particular through the implementation of access logs.

However, the security of data can firstly and foremost be enhanced by informing the data subject in an adequate manner. Only when individuals are informed about what happens when they provide personal data to Internet providers and other entities can the security of personal data be enhanced. Consequently, providing security for personal data is not only about technology, but also about raising awareness by informing the individuals.

19. How can Media and Information Literacy be developed to assist individuals to protect their privacy?

UNESCO's mission to empower people by providing them with access to information and knowledge can be seen as essential for the promotion of the right to privacy and the people's awareness of it. The personal data provided by data subjects has a direct influence on their privacy. It is essential that the individuals are aware of this fact so that they can control and foresee what happens with their personal data (who obtains it, etc.) in order to be able to protect their own privacy. The MIL mission of UNESCO with its different programmes should especially focus on young generations which grow up using the Internet. Education in schools about privacy risks online and what to do to protect their privacy, as well as training teachers are important. This could be included in the UNESCO Global MIL Assessment Framework and be one of the fundamental aims of the MIL mission.

D. Questions related to the field of Ethics

20.How can ethical principles based on international human rights advance accessibility, openness, and multi-stakeholder participation on the Internet?

In the cultural field, ethical principles such as the right to access through inter alia MIL or a right to fair use of existing artistic and cultural material could open up cultural creation to a wider number of citizens, by improving their skills, as well as giving them access to a wider range of material to be able to create, bringing in people to participate in the cultural field who in a more traditional setting would not be there.

22. How does ethical consideration relate to gender dimensions of the Internet?

Ethical considerations are very much a part of the gender dimension of the Internet, as women are generally a vulnerable group for reasons including: (i) stereotyping of women on internet; (ii) objectification of women on internet; (iii) trafficking in human beings, prostitution.

Studies show the right to access and participate is affected by the gender dimension. The right to privacy of certain data may be more important for one gender than the other in different situations.

E. Broader issues

24. What international, regional and national frameworks, normative guidelines and accountability mechanisms exist of relevance to one or more fields of the study?

List of Committee of Ministers Recommendations, Resolutions and Declarations adopted in the media field:

- Declaration of the Committee of Ministers on the protection of journalism and safety of journalists and other media actors (Adopted by the Committee of Ministers on 30 April 2014 at the 1198th meeting of the Ministers' Deputies)

- Recommendation CM/Rec(2013)1 of the Committee of Ministers to member States on gender equality and media (Adopted by the Committee of Ministers on 10 July 2013 at the 1176th meeting of the Ministers' Deputies)

- Declaration of the Committee of Ministers on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies (Adopted by the Committee of Ministers on 11 June 2013 at the 1173rd meeting of the Ministers' Deputies)

- Declaration of the Committee of Ministers on the Desirability of International Standards dealing with Forum Shopping in respect of Defamation, "Libel Tourism", to ensure Freedom of Expression (Adopted by the Committee of Ministers on 4 July 2012 at the 1147th meeting of the Ministers' Deputies)

- Strategy on Internet Governance 2012-2015 of the Committee of Ministers adopted 14 March 2012.

- Recommendation CM/Rec(2012)4 of the Committee of Ministers to member States on the protection of human rights with regard to social networking services (Adopted by the Committee of Ministers on 4 April 2012 at the 1139th meeting of the Ministers' Deputies)

- Recommendation CM/Rec(2012)3 of the Committee of Ministers to member States on the protection of human rights with regard to search engines (Adopted by the Committee of Ministers on 4 April 2012 at the 1139th meeting of the Ministers' Deputies)

- Declaration of the Committee of Ministers on Public Service Media Governance (Adopted by the Committee of Ministers on 15 February 2012 at the 1134th meeting of the Ministers' Deputies)

- Recommendation CM/Rec(2012)1 of the Committee of Ministers to member States on public service media governance (Adopted by the Committee of Ministers on 15 February 2012 at the 1134th meeting of the Ministers' Deputies)

- Declaration of the Committee of Ministers on the protection of freedom of expression and freedom of assembly and association with regard to privately operated Internet platforms and online service providers, adopted on 7 December 2011

- Declaration by the Committee of Ministers on Internet governance principles, adopted on 21 September 2011

- Declaration by the Committee of Ministers on the protection of freedom of expression and information and freedom of assembly and association with regard to Internet domain names and name strings, adopted on 21 September 2011

- Recommendation CM/Rec(2011)7 of the Committee of Ministers to member states on a new notion of media, adopted on 21 September 2011

- Recommendation CM/Rec(2011)8 of the Committee of Ministers to member states on the protection and promotion of the universality, integrity and openness of the Internet, adopted on 21 September 2011

- Declaration of the Committee of Ministers on the management of the Internet protocol address resources in the public interest, adopted on 29 September 2010

- Declaration of the Committee of Ministers on network neutrality, adopted on 29 September 2010

- Declaration of the Committee of Ministers on the Digital Agenda for Europe, adopted 29 September 2010

- Declaration of the Committee of Ministers on enhanced participation of member states in Internet governance matters – Governmental Advisory Committee (GAC) of the Internet Corporation for Assigned Names and Numbers (ICANN), adopted on 26 May 2010

- Declaration of the Committee of Ministers on measures to promote the respect of Article 10 of the European Convention on Human Rights, adopted on 13 January 2010

- Recommendation CM/Rec(2009)5 of the Committee of Ministers to member states on measures to protect children against harmful content and behaviour and to promote their active participation in the new information and communications environment, adopted on 8 July 2009

- Declaration of the Committee of Ministers on the role of community media in promoting social cohesion and intercultural dialogue, adopted on 11 February 2009

- Recommendation CM/Rec(2008)6 of the Committee of Ministers to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters, adopted on 26 March 2008

- Declaration of the Committee of Ministers on the independence and functions of regulatory authorities for the broadcasting sector, adopted by the Committee of Ministers on 26 March 2008

- Declaration on protecting the dignity, security and privacy of children on the internet, adopted on 20 February 2008

- Declaration on the allocation and management of the digital dividend and the public interest, adopted on 20 February 2008

- Recommendation CM/Rec(2007)16 of the Committee of Ministers to member states on measures to promote the public service value of the Internet, adopted on 7 November 2007

- Recommendation CM/Rec(2007)15 of the Committee of Ministers to member states on measures concerning media coverage of election campaigns, adopted on 7 November 2007

- Recommendation CM/Rec(2007)11 of the Committee of Ministers to member states on promoting freedom of expression and information in the new information and communications environment, adopted on 26 September 2007

- Guidelines of the Committee of Ministers of the Council of Europe on protecting freedom of expression and information in times of crisis, adopted on 26 September 2007

- Declaration by the Committee of Ministers on the protection and promotion of investigative journalism, adopted on 26 September 2007

- Recommendation Rec(2007)3 of the Committee of Ministers to member states on the remit of public service media in the information society, adopted on 31 January 2007

- Recommendation Rec(2007)2 of the Committee of Ministers to member states on media pluralism and diversity of media content , adopted on 31 January 2007

- Declaration of the Committee of Ministers on protecting the role of the media in democracy in the context of media concentration, adopted on 31 January 2007

- Recommendation Rec(2006)12 of the Committee of Ministers to member states on empowering children in the new information and communications environment, adopted by the Committee of Ministers on 27 September 2006

- Declaration of the Committee of Ministers on the guarantee of the independence of public service broadcasting in the member states, adopted on 27 September 2006

- Declaration of the Committee of Ministers on human rights and the rule of law in the Information Society (CM(2005)56 final)

- Recommendation Rec(2006)3 of the Committee of Ministers to member states on the UNESCO Convention on the protection and promotion of the diversity of cultural expressions

- Declaration on freedom of expression and information in the media in the context of the fight against terrorism, adopted on 2 March 2005

- Recommendation Rec(2004)16 of the Committee of Ministers to member states on the right of reply in the new media environment

- Declaration on freedom of political debate in the media, adopted on 12 February 2004

- Recommendation No. R (2003) 13 on the provision of information through the media in relation to criminal proceedings

- Declaration on the provision of information through the media in relation to criminal proceedings adopted on 10 July 2003

- Political message from the Committee of Ministers to the World Summit on the Information Society (WSIS)

- Declaration on freedom of communication on the Internet, adopted on 28 May 2003 (PDF version including explanatory note)

- Recommendation No. R (2003) 9 on measures to promote the democratic and social contribution of digital broadcasting

- Recommendation No. R (2002) 7 on measures to enhance the protection of the neighbouring rights of broadcasting organisations

- Recommendation No. R (2002) 2 on access to official documents and Explanatory memorandum

- Recommendation No. R (2001) 8 on self-regulation concerning cyber content and its Explanatory Memorandum

- Recommendation No. R (2001) 7 on measures to protect copyright and neighbouring rights and combat piracy, especially in the digital environment

- Recommendation No. R (2000) 23 on the independence and functions of regulatory authorities for the broadcasting sector and its Explanatory Memorandum

- Recommendation No. R (2000) 7 on the right of journalists not to disclose their sources of information and its Explanatory Memorandum

- Declaration on cultural diversity adopted on 7 December 2000

- Recommendation No. R (99) 15 on measures concerning media coverage of election campaigns and its Explanatory Memorandum

- Declaration on the exploitation of protected radio and television productions held in the archives of broadcasting organisations adopted on 9 September 1999

- Declaration on a European policy for new information technologies adopted on 7 May 1999

- Recommendation No. R (99) 14 on universal community service concerning new communication and information services and its Explanatory Memorandum

- Recommendation No. R (99) 5 for the protection of privacy on the Internet

- Recommendation No. R (99) 1 on measures to promote media pluralism and its Explanatory Memorandum

- Recommendation No. R (97) 21 on the media and the promotion of a culture of tolerance and its Explanatory Memorandum

- Recommendation No. R (97) 20 on "hate speech" and its Explanatory Memorandum

- Recommendation No. R (97) 19 on the portrayal of violence in the electronic media and its Explanatory Memorandum

- Resolution (97) 4 confirming the continuation of the European Audio-visual Observatory

- Recommendation No. R (96) 10 on the guarantee of the independence of public service broadcasting and its Explanatory Memorandum

- Declaration on the protection of journalists in situations of conflict and tension adopted on 3 May 1996

- Recommendation No. R (96) 4 on the protection of journalists in situations of conflict and tension

- Recommendation No. R (95) 13 concerning problems of criminal procedural law connected with information technology

- Recommendation No. R (95) 1 on measures against sound and audio-visual piracy and its Explanatory Memorandum

- Recommendation No. R (94) 13 on measures to promote media transparency and its Explanatory Memorandum

- Declaration on neighbouring rights adopted on 17 February 1994

- Recommendation No. R (94) 3 on the promotion of education and awareness in the area of copyright and neighbouring rights concerning creativity and its Explanatory Memorandum

- Recommendation No. R (93) 5 containing principles aimed at promoting the distribution and broadcasting of audio-visual works originated in countries or regions with a low audio-visual output or a limited geographic or linguistic coverage on the European television markets" and its Explanatory Memorandum

- Resolution (92) 70 on establishing a European Audiovisual Observatory

- Recommendation No. R (92) 19 on video games with a racist content

- Recommendation No. R (92) 15 concerning teaching, research and training in the field of law and information technology and its Explanatory Memorandum

- Resolution (92) 3 modifying Resolution (88) 15

- Recommendation No. R (91) 14 on the legal protection of encrypted television services and its Explanatory Memorandum

- Recommendation No. R (91) 5 on the right to short reporting on major events where exclusive rights for their television broadcast have been acquired in a transfrontier context and its Explanatory Memorandum

- Recommendation No. R (90) 11 on principles relating to copyright law questions in the field of reprography and its Explanatory Memorandum

- Recommendation No. R (90) 10 on cinema for children and adolescents

- Recommendation No. R (89) 7 concerning principles on the distribution of videograms having a violent, brutal or pornographic content and its Explanatory Memorandum

- Resolution (89) 6 modifying Resolution (88) 15

- Resolution (88) 15 setting up a European support fund for the co-production and distribution of creative cinematographic and audiovisual works (“Eurimages”)

- Recommendation No. R (88) 2 on measures to combat piracy in the field of copyright and neighbouring rights

- Recommendation No. R (88) 1 on sound and audiovisual private copying

- Recommendation No. R (87) 7 on film distribution in Europe

- Recommendation No. R (86) 14 on the drawing up of strategies to combat smoking, alcohol and drug dependence in co-operation with opinion-makers and the media

- Recommendation No. R (86) 9 on copyright and cultural policy

- Recommendation No. R (86) 3 on the promotion of audio-visual production in Europe

- Recommendation No. R (86) 2 on principles relating to copyright law questions in the field of television by satellite and cable

- Recommendation No. R (85) 8 on the conservation of the European film heritage

- Recommendation n° R (85) 6 on aid for artistic creation

- Recommendation No. R (84) 22 on the use of satellite capacity for television and sound radio

- Recommendation No. R (84) 17 on equality between women and men in the media

- Recommendation No. R (84) 3 on principles on television advertising

- Declaration on freedom of expression and information adopted on 29 April 1982

- Recommendation No. R (81) 19 on the access to information held by public authorities

- Recommendation No. R (80) 1 on sport and television

- Recommendation No. R (79) 1 concerning consumer education of adults and consumer information

- Resolution (74) 43 on press concentrations

- Resolution (74) 26 on the right of reply - position of the individual in relation to the press

- Resolution (70) 19 on educational and cultural uses of radio and television in Europe and the relations in this respect between public authorities and broadcasting organisations

- Resolution (67) 13 on the press and the protection of youth

- Resolution (61) 23 on the exchange of television programmes