Steering Committee on Media and Information Society - CDMSI

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

CDMSI(2015)021rev
11/12/2015

9th meeting of Steering Committee on Media and Information Society (CDMSI)

08-11 December 2015
(Strasbourg, Palais de l'Europe, Room 08)

Abridged meeting report

The CDMSI held its 9th meeting from 8 to 11 December 2015, in Strasbourg chaired by Ms Maja Raković (Serbia). The CDMSI adopted the agenda as it is set out in Appendix I with one addition i.e. sub-item 7.6. Human rights guidelines for Internet service providers. The list of participants appears in Appendix II. Gender distribution: 60 attendants, 20 women (33%), 40 men (67%).

Items submitted to the Committee of Ministers for decision

The CDMSI finalised and agreed to transmit to the Committee of Ministers for possible adoption the draft Recommendation CM/Rec__of the Committee of Ministers to member States on safety of journalists and other media actors (Appendix III). The Russian Federation wishes to refrain from supporting this draft recommendation and made a statement that will be reflected in the meeting report.

The CDMSI finalised and agreed to transmit to the Committee of Ministers for possible adoption the draft Recommendation CM/Rec__of the Committee of Ministers to member States on Internet freedom (Appendix IV). It also took note of the explanatory memorandum to the draft recommendation, which will be transmitted to the Committee of Ministers to be taken note of. The Russian Federation wishes to refrain from supporting this draft recommendation and made a statement that will be reflected in the meeting report.

The CDMSI finalised and agreed to transmit to the Committee of Ministers for possible adoption the draft Council of Europe Internet Governance Strategy 2016-2019 (Appendix V). The Russian Federation does not approve of the draft Council of Europe Internet Governance Strategy 2016-2019 in its present version and made a statement that will be reflected in the meeting report.

Items submitted to the Committee of Ministers for information

The CDMSI noted the adoption by the Committee of Ministers of its new terms of reference for 2016-2017, as well as the terms of references for two subordinate Committees of experts, respectively on media pluralism and transparency of media ownership (MSI-MED), and on Internet intermediaries (MSI-NET). The CDMSI discussed and voted on the respective member State representatives to participate in MSI-MED and MSI-NET. It noted that, pursuant to their terms of reference, the independent experts will be appointed by the Secretary General. The compositions of the two expert committees appear in appendix VI and VII respectively.

Pursuant to Resolution (2011)24 of the Committee of Ministers on intergovernmental committees and subordinate bodies, their terms of reference and working methods, the CDMSI

elected its Bureau as follows: Ms Elfa Ýr Gylfadóttir, Chair (Iceland), Mr Emir Povlakić, Vice-Chair (Bosnia and Herzegovina) for a first term of office expiring on 31 December 2016, Ms Joanna Chansel (France), Ms Pien van den Eijnden (Netherlands), Mr Matthias Traimer (Austria) Ms Maja Raković (Serbia) for a first two year term of office expiring on 31 December 2017 and Mr. Christopher Lärkner (Sweden) for a first one year term of office expiring on 31 December 2016. It also confirmed Ms Maja Zarić (Serbia) as Gender equality rapporteur.

***

In addition, the CDMSI dealt with the items below:

The CDMSI congratulated the Secretariat on the conference "Freedom of expression – still a precondition for democracy?", held in Strasbourg on 13 and 14 October 2015.

The CDMSI took note of:

- the information given by Mr Jan Kleijssen, Director of Information Society and Action against Crime, in particular on actions undertaken by the Council of Europe following the recent terrorist attacks in Paris and other places;

- information on the state of play of the Recommendation CM/Rec(2015)xxx on protecting the right to freedom of expression and the right to private life with regard to network neutrality;

- 24 replies sent by member states to a questionnaire on safety of journalists and of an analysis prepared by the secretariat. It decided that the outstanding replies should be sent to the secretariat by 29th February 2016. It agreed to hold, at its 10th meeting in June 2016, a hearing on the topic. This should be combined with a presentation and discussion of the Internet based platform on safety of journalists and a first reflection on how to implement the draft recommendation to be submitted to the CM for possible adoption on the protection of journalism and safety of journalists and other media actors. It also agreed that major developments in members states, in particular related to Internet should be shared with members and communicated to the Secretariat.

- the report on Freedom of Assembly and Association on the Internet prepared by the Committee of Experts on cross-border flow of Internet traffic (MSI-INT), which was one of its expected results;

- reports of the last meetings of the MSI-INT and Committee of experts on protection of journalism and safety of journalists (MSI-JO) and congratulated the Committees for the work accomplished in the course of their mandate;

- information on the state of play of the Council of Europe Internet Governance Strategy 2012-2015 and commended the work accomplished, looking forward to the Secretary General's final report;

- information provided by the Secretariat and members who participated in the Internet Governance Forum 2015 that took place in Joao Pessoa, Brazil (10-13/11/2015), as well as of information on the 2016 edition of the European Dialogue on Internet Governance (EuroDIG) that will take place in Brussels (9-10 June 2016);

- information provided by the Secretariat on the state of play of the modernisation of Convention 108 and on-going work of the T-PD on personal data in the police sector, health data, big data and passengers name records;

- information on progress of the drafting committee on Public Service Media that was set up at the last plenary meeting in June 2015 ; having regard to the new mandate of the CDMSI, decided that the discussions should be continued in the MSI-MED;

- information provided by the UK delegate regarding the 54th meeting of ICANN (8-22 October 2015) and the review of the outcomes of the World Summit on Information Society (WSIS). It discussed a suggestion by the UK delegate to encourage the Council of Europe in undertaking research analysis of the human rights matters related to freedom of expression dealt within the Governmental Advisory Committee in ICANN;

- evaluation undertaken by the Council of Europe Directorate of Internet Oversight on the participation of NGOs in steering committees;

- issue paper published by the Council of Europe Commissioner for Human Rights on democratic and effective oversight of national security services;

- information provided by the Secretariat and CDMSI members on a number of activities, meetings and events relating to media and Internet issues;

- following an invitation by the CODEXTER to participate in its work on special investigation techniques, the CDMSI nominated Ms Maja Raković to take part in the CODEXTER drafting group on the topic;

- took note of information on on-going and future co-operation activities.

The CDMSI discussed and emphasised the relevance of up-dating the 2008 Guidelines on human rights for Internet service providers and proposed that this item be put on the agenda of the first meeting of MSI-NET for further discussion.

APPENDIX I
Meeting agenda

1. Opening of the meeting

2. Adoption of the agenda

3. Information by the Chair and the Secretariat

3.1 Draft Recommendation CM/Rec(2014)___of the Committee of Ministers to member States on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality
3.2 Council of Europe Conference on "Freedom of Expression – still a precondition for democracy?" – Strasbourg, 13-14 October 2015
3.3 New mandate of the CDMSI

4. Implementation of Council of Europe adopted standards

5. Media standard setting

5.1 Committee of experts on protection of journalism and safety of journalists (MSI-JO)

6. Internet standard setting

6.1 Committee of Experts on cross-border flow of Internet traffic and Internet freedom (MSI-INT)

7. Internet governance

7.1 Council of Europe Internet Governance Strategy 2012-2015
7.2 Council of Europe Internet Governance Strategy 2016-2019
7.3 European Dialogue on Internet Governance and Internet Governance Forum (João Pessoa, Brazil, on 10-13 November 2015)
7.4. Governmental Advisory Committee (GAC) of the Internet Corporation for Assigned Names and Numbers (ICANN)
7.5. Review of the outcomes of the World Summit on the Information Society (WSIS)

8. Data protection

9. Co-operation activities

10. CDMSI work programme and working methods

10.1 Drafting committees
10.2 Evaluation of NGOs participation in Steering Committees

11. Information about the work of other organisations and other Council of Europe bodies

11.1 Parliamentary Assembly of the Council of Europe (PACE)
11.2 Commissioner for Human Rights
11.3. CODEXTER

12. Representation of CDMSI in meetings of other committees and events

13. Elections

14. Any other business

15. **Abridged report of the 9th meeting**

APPENDIX II

LIST OF PARTICIPANTS / *LISTE DES PARTICIPANTS*

9TH MEETING OF THE STEERING COMMITTEE ON MEDIA AND INFORMATION SOCIETY
9EME REUNION DU COMITE DIRECTEUR SUR LES MEDIAS ET LA SOCIETE DE L'INFORMATION (CDMSI)

8 – 11 DECEMBER / *DECEMBRE 2015*
ROOM/SALLE 8 (PALAIS DE L'EUROPE)

ALBANIA / ALBANIE
Mr Glevin Dervishi
Adviser on Media to the Albanian Minister of Foreign Affairs, Ministry of Foreign Affairs

ARMENIA / ARMENIE
Ms Shahane Hakobyan
Department for Relations with European Court of Human Rights, Ministry of Justice of the Republic of Armenia

AUSTRIA / AUTRICHE
Mr Matthias Traimer
Federal Chancellery, Media Affairs and Information Society, Federal Chancellery, Constitutional Service

AZERBAIJAN
Ms Jeyran Amiraslanova
Senior Adviser of the Administration of the President

BOSNIA AND HERZEGOVINA / BOSNIE-HERZEGOVINE
Mr Emir Povlakić
Head of Division for Licensing, Digitalization and Coordination in Broadcasting, Communications Regulatory

CROATIA / CROATIE
Mr Milan F. Zivković
Head Advisor for Communication Policy, Ministry of Culture

DENMARK / DANEMARK
Ms Katja Just Maarbjerg
Ministry of Culture

ESTONIA / ESTONIE
Dr. Indrek Ibrus
Associate Professor, Tallinn University, Baltic Film and Media School

FRANCE
Ms Joanna Chansel
Bureau des affaires européennes et internationales, Direction Générale des Médias et des Industries Culturelles
Ministère de la Culture et de la Communication

M. Julien Plubel
Rédacteur
Ministère des Affaires étrangères, Direction de la coopération culturelle, universitaire et de la recherche, Pôle de l'audiovisuel extérieur

GEORGIA / GEORGIE
Ms Irine Bartaia

Deputy Director, Department of International Law, Ministry of Foreign Affairs of Georgia

GERMANY / ALLEMAGNE
Mr Gajus Köhr (8, 9, 10, 11 December)
Division K 31, International Media Cooperation, Federal Government Commissioner for Culture and the Media

Mr Jan Wiegandt (8-9 Dec)
Representation of the State of Rhineland-Palatinate to the EU

Ms Annick Kuhl (10-11 Dec)
Representation of the Free State of Bavaria to the EU

GREECE / GRECE
Mr Evangelos Valmas
Deputy Director of the Directorate for Mass Media
Head of the Department for Audiovisual Media & Archives
Secretariat General for Information & Communication

HUNGARY / HONGRIE
Mr György Ocskó
International Legal Adviser, National Media and Infocommunications Authority

ICELAND / ISLANDE
Ms Elfa Ýr Gylfadóttir
Media Commission, Ministry of Education, Science and Education

IRELAND / IRLANDE
Mr Éanna O'Conghaile
Principal Officer, Broadcasting Policy Division, Department of Communications, Energy & Natural Resources

ITALY / ITALIE
Mr Pierluigi Mazzella
Director General, Agency for the right to university education, Professor of Information and Communication, University of Rome

LATVIA / LETTONIE
Mr Andris Mellakauls
Information Space Integration, Ministry of Culture

LIECHTENSTEIN
Mr Claudio Nardi
Officer for Foreign Affairs

MOLDOVA / MOLDOVIE
Mr Serghei Mihov
Counsellor , Global Affairs and Human Rights Division , General Directorate for Multilateral Cooperation, Ministry of Foreign Affairs and European Integration of the Republic of Moldova

MONACO
M. Serge Robillard
Chef de Division, Direction des Communications Électroniques, Principauté de Monaco

MONTENEGRO
Mr Ranko Vujović, Executive Director, UNEM

THE NETHERLANDS / PAYS-BAS
Mr Nol Reijnders

Senior Adviser for Media Policy

Ms Pien van den Eijnden
Senior legal adviser
Ministry of the Interior and Kingdom Relations, Constitutional Affairs and Legislation, Constitutional Affairs

NORWAY / NORVEGE
Mr Olav Guntvedt
Assistant Director General, Department of Media Policy and Copyright, Ministry of Culture

POLAND / POLOGNE
Ms Małgorzata Pek
Deputy director, Strategy Department, National Broadcasting Council of Poland

ROMANIA / ROUMAIE
Ms Delia Mucica
Professor, University of Theatre and Film
Senior Advisor, Unit for Project Management, Ministry of Culture and National Heritage

RUSSIAN FEDERATION / FEDERATION RUSSIE
Mr Alexander Surikov
Deputy Director Department of Information and Press, Ministry of Foreign Affairs

Mr.Arseny Nedyak

Mr.Nadzhaf Abdullaev

SAN MARINO / SAINT MARIN
Mme Chiara Cardogna
Agent de presse - Département des Affaires Etrangères

SERBIA / SERBIE
Ms Maja Raković (Chair / Président)
First Counselor, Serbian Embassy, France

Ms Maja Zarić
Adviser, Sector for International Relations, EU integration and projects, Ministry of Culture and Information

SLOVENIA / SLOVENIE
Mr Skender Adem
Undersecretary, Ministry of Culture of Republic of Slovenia

SLOVAKIA / SLOVAQUIE
Ms Ivana Maláková
Head of Unit Media Law and Audiovisual Unit Media, Audiovisual and Copyright Department
Ministry of Cultura of Slovak Republic

SWEDEN
Mr Christoffer Lärkner
Department of Culture

SWITZERLAND / SUISSE
Mr Frédéric Riehl
Federal Office of Communication, Federal Department for the environment, transport, energy and communication

Mr Thomas Schneider

International Affairs, Federal Office of Communication, Federal Department for the environment, transport, energy and communication
„FORMER YUGOSLAV REPUBLIC OF MACEDONIA „/ „*EX-REPUBLIQUE YOUGOSLAVE DE MACEDOINE*"
Ms Vesna Poposka
Head of International PR Department, Government of the Republic of Macedonia, PR Department

TURKEY / TURQUIE
Mr Mehmet Bora Sönmez
Media Expert, Radio and Television Supreme Council of Turkey

Mr Ahmet Yanik
Assistant Expert

Mr Ahmet Kilic
Head of Department, Information and Communication Technology Authority

Mr Lufti Gunenez
Expert, Information and Communication Technology Authority

UKRAINE
Ms Olha Herasymiuk
First Deputy Chair of the National Council of Ukraine for Television and Radio Broadcasting

UNITED KINGDOM / ROYAUME-UNI
Mr Mark Carvell
Media Team, Department for Culture, Media and Sport

* * *

OBSERVERS and PARTICIPANTS / *OBSERVATEURS et PARTICIPANTS*

BELARUS
Mr Dimintry Mironchik
Head of Media Department of MFA Belarus, Press-Secretary of MFA

EUROPEAN BROADCASTING UNION (EBU)
Ms Anne-Catherine Berg

EAVI
Mr Paolo Celo
Director and Secretary General, European Association for Viewers Interests

EUROPEAN AUDIOVISUAL OBSERVATORY / OBSERVATOIRE EUROPPENNE DE L'AUDIOVISUAL
Ms Susanne Nikoltchev
Executive Director

EuroISPA
Mr Michael Rotert
Honorary Spokesman

ASSOCIATION OF EUROPEAN JOURNALISTS (AEJ) / MEDIA FREEDOM REPRESENTATIVE
Mr William Horsley
Media Freedom Representative

CONFERENCE OF INTERNATIONAL NON-GOVERNMENTAL ORGANISATIONS OF THE COUNCIL OF EUROPE / CONFÉRENCE DES ORGANISATIONS INTERNATIONALES NON GOUVERNEMENTALES DU CONSEIL DE L'EUROPE

Mr Didier Schretter
Member of the Standing Committee, Vice-chair Education and Culture Committee
HOLY SEE / SAINT SIEGE
Dr Michael Lukas
Episcopal Press Office

INTERNET WATCH FOUNDATION
Mr Kristof Claesen
Press and Public Affairs Manager

ICANN
Mr Nigel Hickson (Weds)
VP, UN and IGO Engagement

EUROPEAN COMMISSION
Mr Maciej TOMASZEWSKI
European Commission / DG-CONNECT

OFFICE OF THE COMMISSIONER FOR HUMAN RIGHTS
Ms Alessandra Ricci
Adviser to the Commissioner

PARLIAMENTARY ASSEMBLY OF THE COUNCI OF EUROPE / ASSEMBLEE PARLEMENTAIRE DU CONSEIL DE L'EUROPE
Mr Rüdiger Dossow
Secretary of the Committee on Culture, Science and Education

COUNCIL OF EUROPE EUROPEANCOMMITTEE ON LEGAL CO-OPERATION (CDCJ)
M. Maciej Lewandowski
Member

ADVISORY COUNCIL ON YOUTH OF THE COUNCIL OF EUROPE
Mr Gian Piero Carlo Milani
Member of the Advisory Council on Youth of the Council of Europe

PERMANENT REPRESENTATION OF BELGIUM TO THE COUNCIL OF EUROPE
M Jean Zamani
Research Assistant, Information Society

PERMANENT REPRESENTATION OF LUXEMBOURG TO THE COUNCIL OF EUROPE
Mr Mattia Leveghi
Interne

PERMANENT REPRESENTATION OF LUXEMBOURG TO THE COUNCIL OF EUROPE
Ms Stéphanie Toschi
Interne

PERMANENT MISSION OF MEXICO TO THE COUNCIL OF EUROPE
M. Diego Sandova Pimentel
Adjoint à l'Observateur Permanent du Mexique

* * *
INTERPRETERS / INTERPRETES
Ms Amanda Beddows
Ms Martine Caraly
M Nicolas Guittonneau
Ms Gillian Wakenhut
* * *

SECRETARIAT

Mr Jan Kleijssen, Director of Information Society and Action against Crime, Directorate General Human Rights and Rule of Law
Mr Patrick Penninckx, Head of Information Society Department, Directorate General Human Rights and Rule of Law
Ms Silvia Grundmann, Head of Media and Internet Division, Directorate General of Human Rights and Rule of Law, Secretary to the CDMSI
Ms Onur Andreotti, Administrator, Media and Internet Division, Directorate General Human Rights and Rule of Law
Ms Lejla Dervisagic, Administrator, Media and Internet Division, Directorate General Human Rights and Rule of Law
Ms Ana Gascón Marcén, Administrator, Media and Internet Division, Directorate General Human Rights and Rule of Law
Mr Lee Hibbard, Administrator, Media and Internet Division, Directorate General Human Rights and Rule of Law
Ms Elvana Thaçi, Administrator, Media and Internet Division, Directorate General Human Rights and Rule of Law
Ms Anne Boyer-Donard, Principal Administrative Assistant, Media and Internet Division, Directorate General Human Rights and Rule of Law
Ms Julia Whitham, Assistant, Media and Internet Division, Directorate General Human Rights and Rule of Law
Ms Saskia De Vos, Intern, Media and Internet Division, Directorate General Human Rights and Rule of Law

APPENDIX III

Draft Recommendation CM/Rec(2015)__ of the Committee of Ministers to member states on the protection of journalism and safety of journalists and other media actors

(adopted by the Committee of Ministers on ____ 2015 at the __th meeting of the Ministers' Deputies)

1. It is alarming and unacceptable that journalists and other media actors in Europe are increasingly being threatened, harassed, subjected to surveillance, intimidated, arbitrarily deprived of their liberty, physically attacked, tortured and even killed because of their investigative work, opinions or reporting, particularly when their work focuses on the misuse of power, corruption, human rights violations, criminal activities, terrorism and fundamentalism. These abuses and crimes have been extensively documented in authoritative reports published by the media, non-governmental organisations and human rights defenders.

2. Journalists and other media actors are often specifically targeted on account of their gender, gender identity, sexual orientation, ethnic identity, membership of a minority group, religion, or other particular characteristics, which may expose them to discrimination and dangers in the course of their work. Female journalists and other female media actors face specific gender-related dangers, including sexist, misogynist and degrading abuse; threats, intimidation and harassment and sexual aggression and violence. These violations are increasingly taking place online. There is a need for urgent, resolute and systemic responses.

3. The abuses and crimes described above, which in practice are committed by state and non-state actors, have a grave chilling effect on freedom of expression, as safeguarded by Article 10 of the European Convention on Human Rights, including on the ability to access information, on the public watchdog role of journalists and other media actors and on open and vigorous public debate, all of which are essential in a democratic society. They are often met with insufficient efforts by relevant State authorities to bring the perpetrators to justice, which leads to a culture of impunity, and can fuel further threats and violence and undermine public trust in the rule of law.

4. This alarming situation is not exclusively limited to professional journalists and other traditional media actors. As the European Court of Human Rights has recognised, as well as many intergovernmental bodies, including the United Nations in its Plan of Action on the Safety of Journalists and the Issue of Impunity and in the Human Rights Committee's General Comment No. 34, the scope of media actors has expanded as a result of new forms of media in the digital age. It also, therefore, includes others who contribute to public debate and who perform journalistic activities or public watchdog functions.

5. Given the scale and severity of threats and attacks against journalists and other media actors in Europe and their damaging effects on the functioning of democratic society, far-reaching measures are necessary at the international and national levels in order to strengthen the protection of journalism and the safety of journalists and other media actors, and to eradicate impunity. The international community has repeatedly stated the need for a more effective implementation of existing international and regional standards and an enhanced compliance with existing reporting mechanisms and initiatives. The protection of journalists and other media actors and combatting impunity for perpetrators of crimes against them are pressing political priorities across Council of Europe member States, as stated in the Declaration of the Committee of Ministers on the protection of journalism and safety of journalists and other media actors.

6. In order to create and secure a favourable environment for freedom of expression guaranteed by the Article 10 of the ECHR , states must fulfil a range of positive obligations, as identified and developed by the European Court of Human Rights and set out in the Principles appended to this Recommendation. Such obligations are to be fulfilled by the executive, legislative and judicial branches of governments, as well as all other states authorities,

including agencies concerned with maintaining public order and national security, and at all levels – federal, national, regional and local.

7. Under the terms of Article 15.*b* of the Statute of the Council of Europe, the Committee of Ministers recommends that governments of member states as a matter of urgency and taking full account of the Principles appended to the present Recommendation:

(i) Fulfill the range of their obligations, negative and positive, in letter and in spirit;

(ii) Implement, through all branches of State authorities, the Guidelines set out below;

(iii) Review relevant domestic laws and practice and revise them, as necessary, to ensure their conformity with states' obligations under the European Convention on Human Rights;

(iv) Promote the goals of this Recommendation at the national level and engage and cooperate with all interested parties to achieve those goals.

GUIDELINES

These Guidelines are designed to meet the many-sided challenge of ensuring effective protection of journalism and safety of journalists and other media actors, which necessitates coherent, complementary strategies by member states. They are based on the Principles that are set out in the Appendix and which constitute an integral part of the Recommendation. The Guidelines are organised into four pillars: prevention, protection, prosecution (including a specific focus on impunity) and promotion of information, educational and awareness-raising measures. Within each pillar, detailed guidance is offered to member states on how to fulfil their relevant obligations, combining legal, administrative and practical measures.

Prevention

1. Member states should, in accordance with their constitutional and legislative traditions, ensure independence of the media and safeguard media pluralism, including the independence and sustainability of public service media and community media, which are crucial elements of a favourable environment for freedom of expression.

2. Member states should put in place a comprehensive legislative framework that enables journalists and other media actors to contribute to public debate effectively and without fear. Such a framework should reflect the principles set out in the Appendix to this Recommendation and thereby guarantee public access to information; privacy and data protection; confidentiality and security of communications, and protection of journalistic sources and whistle-blowers. The legislative framework, including criminal-law provisions dealing with the protection of the physical and moral integrity of the person, should be implemented in an effective manner, including through administrative mechanisms and recognising the particular roles of journalists and other media actors in democratic society. The legislative framework and its implementation should guarantee effective protection of female journalists and other female media actors from gender-related dangers in the course of their work. Due attention should be paid to the importance of adequate labour and employment laws to protect journalists and other media actors from arbitrary dismissal or reprisals, and from precarious working conditions that may expose them to undue pressures to depart from accepted journalistic ethics and standards.

3. This legislative framework should be subject to independent, substantive review, to ensure that safeguards for the exercise of the right to freedom of expression are robust and effective in practice and that the legislation is backed up by effective enforcement machinery. After an initial expeditious review, further reviews should be carried out at regular periodic intervals. The reviews of laws and practice should assess the compliance of the legislative framework and its application with authoritative European and international human rights standards, including all relevant positive obligations of states, and make recommendations on the basis of its key findings. The reviews should cover existing and draft legislation, including legislation which concerns terrorism, extremism and national security, and any other legislation that affects the right to freedom of expression of journalists and other media actors as well as other rights that are crucial for ensuring that their right to freedom of expression can be exercised in an effective manner.

4. The reviews may be carried out by one or more appropriate new or existing independent bodies that have authoritative mandates and are supported by sufficient resources. National authorities are urged to establish favourable conditions in which such reviews may take place, allowing for detailed public scrutiny and the drawing up of recommendations by organisations and experts acting independently of governmental, political, religious, commercial and other partisan influences. The reviewing body or bodies could be a national human rights commission, ombudsperson, and/or another independent body established for the specific purposes described. It is recommended that the reviewing body or bodies should have an explicit mandate to seek, receive and use information from any source and be granted optimal access to State documents and officials across all branches of State authorities. The review process should be transparent and include public hearings,

facilitating the full and active participation of civil society, including representatives of journalist organisations, the media and other stakeholders.

5. Provision should be made for the reports of the reviews to be formally submitted to relevant State authorities, including ministries, requiring a timely response by relevant State authorities, including, as appropriate, corrective or other follow-up action to the findings and recommendations of the reviews. The findings and recommendations of the reviews should also be systematically channelled into ongoing reporting, monitoring or information-sharing exercises in the Council of Europe context, such as the Committee of Ministers, the Parliamentary Assembly and the Commissioner for Human Rights. They may also be made available to similar exercises by other intergovernmental organisations, such as the UN Human Rights Committee, the UN Human Rights Council's Universal Periodic Review, UNESCO, the UN High Commissioner for Human Rights and the OSCE Representative on Freedom of the Media.

6. As part of the reviews of laws and practice, member states which have defamation laws should ensure that those laws include freedom of expression safeguards that conform to European and international human rights standards, including truth/public-interest/fair comment defences and safeguards against misuse and abuse, in accordance with the principle of proportionality, as developed by the European Court of Human Rights. Furthermore, given the chilling effect that legislation criminalising particular types of expression has on freedom of expression and public debate, states should exercise restraint in applying such legislation, where it exists. States should be guided in this regard by the European Court of Human Rights' finding that the imposition of a prison sentence for a press offence is only permissible in exceptional circumstances, notably where other fundamental rights have been seriously impaired, as, for example, in the case of hate speech or incitement to violence. Such legislation should be subjected to similar critical scrutiny in the context of the reviews of laws and practices.

7. Member states should clarify the legal bases of State surveillance and interception of communications data and procedural safeguards against misuse and abuse, such as the possibility of review by a competent judicial authority, due process and user notification. Member states should ensure the effective operation of oversight mechanisms for State surveillance of communications, to ensure transparency about the scope and nature of such practices and accountability for the same. Such oversight bodies should have meaningful representation from a range of stake-holders, including journalists and their organisations and legal and technical experts.

Protection

8. Legislation criminalising violence against journalists must be backed up by law enforcement machinery and redress mechanisms for victims (and their families) that are effective in practice. Clear and adequate provision should be made for effective injunctive and precautionary forms of interim protection for those who face threats of violence.

9. State authorities have a duty to prevent or suppress offences against individuals when they know or ought to have known of the existence of a real and immediate risk to the life or physical integrity of an individual or individuals from the criminal acts of a third party and to take measures within the scope of their powers which, judged reasonably, might be expected to avoid that risk. To achieve this, member states should take appropriate preventive operational measures, such as providing police protection, especially when it is requested by journalists or other media actors, or voluntary evacuation to a safe place. Those measures should be effective and timely and should be designed in light of gender-specific dangers faced by female journalists and other female media actors.

10. Member states should encourage the establishment of, and support the operation of, early-warning and rapid response mechanisms, such as hotlines, online platforms or 24-hour emergency contact points, by media organisations or civil society, to ensure that journalists and other media actors, when threatened, have immediate access to protective measures. If established and run by the State, such mechanisms should be subject to meaningful civil

society oversight and guarantee protection for whistle blowers and sources who wish to remain anonymous. Member states are urged to wholeheartedly support and cooperate with the Council of Europe's Platform to promote the protection of journalism and the safety of journalists and thereby help to strengthen the capacity of Council of Europe bodies to warn of and respond effectively to threats and violence against journalists and other media actors.

11. In all cases of deprivation of liberty of journalists or other media actors by police or other law-enforcement officials, adequate procedural guarantees must be adhered to, in order to prevent unlawful detention or ill-treatment. Such procedural guarantees must include: the right to inform, or to have informed, a third party of his/her choice of their deprivation of liberty, of their location and of any transfers; the right of access to a lawyer; the right of access to a medical doctor, and the right to challenge the lawfulness of the detention before a court of law. Persons arrested or detained in relation to the commission of an offence must be brought promptly before a judge, and they have the right to receive a trial within a reasonable time or to be released pending trial, in accordance with Article 5 ECHR (right to liberty and security), as interpreted by the European Court of Human Rights in its case-law.

12. Member states are urged to develop protocols and training programmes for all State authorities with responsibility for fulfilling State obligations concerning the protection of journalists and other media actors. Those protocols should be adapted to the nature and mandate of the State agency in question, for example, the judiciary, prosecutors, police officers, military personnel, prison wardens, immigration officials and other State authorities, as appropriate. The protocols and training programmes should be used to ensure that the personnel of all State agencies are fully aware of the relevant State obligations under international human rights law and humanitarian law and the concrete implications of those obligations for each agency. The protocols and training programmes should be informed by an appreciation of the important roles played by journalists and other media actors in democratic society and of gender-specific issues.

13. Member states must exercise vigilance to ensure that legislation and sanctions are not applied in a discriminatory or arbitrary fashion against journalists and other media actors. They should also take the necessary legislative and/or other measures to prevent the frivolous, vexatious or malicious use of the law and legal process to intimidate and silence journalists and other media actors. Member states should exercise similar vigilance to ensure that administrative measures such as registration, accreditation and taxation schemes are not used to harass journalists and other media actors, or to frustrate their ability to contribute effectively to public debate.

14. Member states should take into account the specific nature and democratic value of the role played by journalists and other media actors in particular contexts, such as in times of crisis, during election periods, at public demonstrations and in conflict zones. In these contexts in particular, it is important for law-enforcement authorities to respect the role of journalists and other media actors covering demonstrations and other events. Press or union cards, relevant accreditation and journalistic insignia should be accepted by state authorities as journalistic credentials, and where it is not possible for journalists or other media actors to produce professional documentation, every possible effort should be made by the state authorities to ascertain their status. Dialogue between state authorities and journalists' organisations is moreover encouraged in order to avoid friction or clashes between police and members of the media.

15. State officials and public figures should not undermine or attack the integrity of journalists and other media actors, for example on the basis of their gender or ethnic identity, or by accusing them of disseminating propaganda and thereby jeopardise their safety. Nor should they require, coerce or pressurize, by way of violence, threats, financial penalties or inducements or other measures, journalists and other media actors to derogate from accepted journalistic standards and professional ethics by engaging in the dissemination of propaganda or disinformation. State officials and public figures should publicly and unequivocally condemn all instances of threats and violence against journalists and other media actors, irrespective of the source of those threats and acts of violence.

16. Member states should encourage media organisations, while not encroaching on their editorial or operational autonomy, to fulfil their institutional responsibilities towards all journalists and other media actors working for them – in salaried, freelance and all other capacities. This may include the adoption of in-house guidelines and procedures for the deployment of journalists and other media actors on difficult or dangerous assignments, for instance in conflict zones. Such deployment should be voluntary and informed. Institutional responsibilities also include providing journalists and other media actors with adequate information and risk-awareness, and requisite training in all matters of safety, digital security and privacy, as well as arranging for life assurance and health and travel insurance as part of a comprehensive and equitable package of work conditions. They additionally include, as relevant, the provision of legal support and representation, and trauma counselling on return from assignments.

Prosecution

17. It is imperative that everyone involved in killings of, attacks on and ill-treatment of journalists and other media actors be brought to justice. Investigations into such crimes and the prosecution of those responsible for them must therefore meet a number of general requirements. When those responsible for such crimes are not brought to justice, a culture of impunity can arise, which calls for particular courses of action.

General requirements

18. Investigations into killings, attacks and ill-treatment must be effective and therefore respect the essential requirements of adequacy, thoroughness, impartiality and independence, promptness and subjection to public scrutiny.

19. Investigations must be effective in the sense that they are capable of leading to the establishment of the relevant facts as well as the identification and eventually, if appropriate, punishment of those responsible. The authorities must take all the reasonable steps to secure all the evidence concerning the incident. The investigation's conclusions must be based on thorough, objective and impartial analysis of all the relevant elements, including the establishment of whether there is a connection between the threats and violence against journalists and other media actors and the exercise of journalistic activities or contributing in similar ways to public debate. State authorities are also obliged to investigate the existence of a possible link between racist attitudes and an act of violence. The relevance of gender-related issues should also be investigated.

20. For an investigation to be effective, the persons responsible for and carrying out the investigation must be independent and impartial, in law and in practice. Any person or institution implicated in any way with a case must be excluded from any role in investigating it. Moreover, investigations should be carried out by specialized, designated units of relevant State authorities in which officials have been given adequate training in international human rights norms and safeguards. Investigations must be effective in order to maintain public confidence in the authorities' maintenance of the rule of law, to prevent any appearance of collusion in or tolerance of unlawful acts and, in those cases involving State agents or bodies, to ensure their accountability for deaths occurring under their responsibility. Investigations should also be subject to public oversight and in all cases, the next of kin of the victim must be involved in the procedure to the extent necessary to safeguard his or her legitimate interests.

21. Member states have an obligation to take all necessary steps to bring the perpetrators of crimes against journalists and other media actors to justice, whether they are State or non-State actors. Investigations and prosecutions should consider all of the different – actual and potential - roles in such crimes, such as authors, instigators, perpetrators and accomplices, and the criminal liability that arises from each of those roles.

22. Member states are obliged to ensure the integrity of court proceedings; they must guarantee the independence and impartiality of the judiciary. They must also ensure the safety

of judges, prosecutors, lawyers and witnesses involved in prosecutions for crimes against journalists and other media actors.

23. Member states must ensure that effective and appropriate remedies are available to victims and, as relevant, to their families, including legal remedies, financial compensation, medical and psychological treatment, relocation and shelter. Remedies should take due account of gender-related, cultural, ethnic, religious and other sensitivities. An ongoing or pending criminal prosecution should not preclude victims from seeking civil remedies.

Impunity

24. When prosecutions for crimes against journalists and other media actors are not initiated or are obstructed in different ways, unacceptable delays are caused to the administration of justice which give rise to impunity for those responsible for the crimes. Therefore, when a State agent has been charged with crimes involving ill-treatment, it is of the utmost importance that criminal proceedings and sentencing are not time-barred. In order to maintain public trust in the justice system, measures such as the granting of an amnesty or pardon should not be envisaged or accepted without convincing reasons. There should be provision by law for additional or aggravated penalties to be applicable to public officials who, by neglect, complicity or design, act in a way that prevents or obstructs the investigation, prosecution or punishment of those responsible for crimes against journalists or other media actors on account of their work or contribution to public debate.

25. When investigations and prosecutions do not result in bringing to justice the perpetrators of killings of, or other serious crimes against, journalists or other media actors, member states may consider establishing special judicial or non-judicial inquiries into specific cases or independent specialised bodies to conduct such inquiries on an ongoing basis. The latter may have special authority and involve participation or leadership by respected media and/or civil society figures, with the aim of advancing the process of fact-finding, without prejudice to the responsibility of the State prosecuting and investigating authorities to bring the perpetrators to justice.

26. Member states should enhance the cooperation and exchange of information, expertise and best practices with other states whenever crimes against journalists and other media actors involve cross-border or online dimensions, subject to safeguards for the rights to privacy, data protection and the presumption of innocence.

27. Member states should pro-actively and vigorously pursue the priorities of protection of journalists and other media actors and combating impunity in all relevant regional and international intergovernmental forums and, more generally, in their foreign policy and relations. This could involve cooperating fully with information-gathering, awareness-raising and other initiatives coordinated by international and regional intergovernmental organisations concerning the safety of journalists and other media actors, in particular periodic state reporting processes, e.g., to the UN Human Rights Committee, as part of the UN Human Rights Council's Universal Periodic Review and to the Director-General of UNESCO on the actions taken to prevent the impunity of perpetrators and on the status of judicial inquiries on each of the killings of journalists condemned by UNESCO. This would also include member states' roles and responsibility in the supervision of the execution of the judgments of the European Court of Human Rights by the Council of Europe's Committee of Ministers and providing prompt and full responses to ad hoc requests by the Council of Europe's Commissioner for Human Rights and the OSCE Representative on Freedom of the Media.

Promotion of information, education and awareness-raising

28. Member states should promote the translation (into the national and minority languages) and the widest possible dissemination of this Recommendation, as well as awareness-raising about its content in a variety of publicity materials. Information and awareness-raising strategies should include specific campaigns designed to capitalise on the publicity opportunities provided by internationally-designated days such as World Press

Freedom Day (3 May), International Day to End Impunity for Crimes against Journalists (2 November) and International Right to Know Day (28 September). Member states should cooperate fully with information-gathering, awareness-raising and other initiatives coordinated by international and regional intergovernmental organisations concerning the safety of journalists and other media actors. In doing so, they should pro-actively highlight, as appropriate, gender-specific issues and other issues concerning impermissible grounds for discrimination.

29. Member states should encourage relevant bodies to give prominence to this Recommendation – and educational materials dealing with all the issues it addresses, including gender-specific issues - in training programmes in journalism schools and as part of ongoing education for journalists, and media and information literacy initiatives.

30. Member states should develop a partnership with civil society and the media for the promotion of best practices for the protection of journalists and other media actors and for combating impunity. This should involve putting into practice the principles of open government and open justice and adopting a constructive and responsive attitude to civil society and media reporting on threats and violence against journalists and other media actors, highlighting gender-specific and other issues, as appropriate. It should also involve active cooperation in publicising and educating about relevant issues and standards.

Appendix

PRINCIPLES

The preceding Recommendation is based on an extensive body of principles, anchored in the European Convention on Human Rights and developed by the European Court of Human Rights in its case-law. A relevant selection of these principles are set out and contextualised in the following paragraphs. The principles have been grouped into the following categories: Freedom of expression; Enabling environment; Safety, security, protection; Contribution to public debate, and Chilling effect.

Freedom of expression

1. The right to freedom of expression, as enshrined in Article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), Article 19 of the Universal Declaration of Human Rights, Article 19 of the International Covenant on Civil and Political Rights and other international and regional instruments, is a fundamental human right enjoyed by everyone, offline and online, without discrimination. It is a compound right, comprising the right to hold opinions and the rights to seek, receive and impart information and ideas of all kinds without interference and regardless of frontiers.

2. The right to freedom of expression and information as guaranteed by Article 10 ECHR constitutes one of the essential foundations of a democratic society and one of the basic conditions for its progress and the development of every individual. Freedom of expression is applicable not only to 'information' or 'ideas' that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population. In this way, freedom of expression facilitates robust public debate, which is another prerequisite of a democratic society characterised by pluralism, tolerance and broadmindedness. Any interference with the right to freedom of expression of journalists and other media actors therefore has societal repercussions as it is also an interference with the right of others to receive information and ideas and an interference with public debate.

3. The exercise of the right to freedom of expression carries with it duties and responsibilities, as stated in Article 10(2). In the context of journalism, relevant duties and responsibilities are understood as including, acting in good faith in order to provide accurate and reliable information, in accordance with the ethics of journalism.

4. While the right to freedom of expression is not absolute, an interference with the right may only be permissible if it is prescribed by law, pursues one of the legitimate aims set out in Article 10(2) ECHR, is necessary in democratic society, which implies that it corresponds to a pressing social need, and is proportionate to the legitimate aim(s) pursued. Those aims are: national security, territorial integrity or public safety, the prevention of disorder or crime, the protection of health or morals, the protection of the reputation or rights of others, preventing the disclosure of information received in confidence, or maintaining the authority and impartiality of the judiciary.

5. Moreover, some types of hate speech which incite to violence or hatred fall under Article 17 ECHR (prohibition of abuse of rights) and are therefore not afforded protection under the Convention because their aim is to destroy some of the rights and freedoms set forth in the Convention.

6. All human rights are universal, indivisible, interdependent and interrelated and, in particular, the right to freedom of expression has important interaction with other human rights, such as the rights to freedom of thought, conscience and religion, the right to freedom of assembly and association and the right to vote in free and fair elections.

7. Other human rights associated with issues surrounding the safety of journalists and other media actors and the fight against impunity include: the right to life (Article 2); the prohibition of torture (Article 3); the right to liberty and security (Article 5); the right to a fair trial (Article 6) and no punishment without law (Article 7); the right to respect for private and family life (Article 8), and the right to an effective remedy (Article 13).

8. The ECHR is a living instrument which is to be interpreted in light of present-day conditions and in a way that ensures that all of the rights it guarantees are not theoretical or illusory but practical and effective, both in terms of the substance of those rights and the remedies available in case of their violation.

9. Ongoing technological developments have transformed the traditional media environment, as described *inter alia* in CM/Rec (2011)7 on a new notion of media, leading to new notions of media and new understandings of the evolving media ecosystem. Advances in information and communication technologies have made it easier for an increasing and increasingly diverse range of actors to participate in public debate. Consequently, the European Court of Human Rights has repeatedly recognised that besides professional journalists and media, individuals, civil society organisations, whistle-blowers and academics can all make valuable contributions to public debate, thereby playing a role similar or equivalent to that traditionally played by the institutionalised media and professional journalists.

10. The UN Human Rights Committee has similarly stated that "journalism is a function shared by a wide range of actors, including professional full-time reporters and analysts, as well as bloggers and others who engage in forms of self-publication in print, on the Internet or elsewhere". The UN General Assembly has also acknowledged that "journalism is continuously evolving to include inputs from media institutions, private individuals and a range of organizations that seek, receive and impart information and ideas of all kinds, online as well as offline […] thereby contributing to shape public debate". According to the UN Plan of Action on the Safety of Journalists and the Issue of Impunity, "the protection of journalists should not be limited to those formally recognised as journalists, but should cover others, including community media workers and citizen journalists and others who may be using new media as a means of reaching their audiences".

11. The obligation on states to ensure the effective exercise of human rights involves not only negative obligations of non-interference, but also positive obligations to secure those rights to everyone within their jurisdiction.

12. Genuine, effective exercise of freedom of expression may require various positive measures of protection, even in the sphere of relations between individuals. Such positive

obligations include, among others: the obligation to create a favourable environment for participation in public debate for everyone and to enable the expression of ideas and opinions without fear; the obligation to put in place an effective system of protection for authors and journalists; the obligation to afford protection against physical violence and intimidation; the obligation to protect life; the obligation to investigate fatalities, and the duty to prevent torture and ill-treatment.

Enabling Environment

13. A favourable or enabling environment for freedom of expression has a number of essential features which collectively create the conditions in which freedom of expression and information and vigorous public debate can thrive. The right to receive information embraces a right of access to information and the public has a right to receive information and ideas of public interest, which journalists and other media actors have the task of imparting. The gathering of information is an essential preparatory step in journalism and an inherent, protected part of press freedom. The participation of journalists and other media actors in public debate on matters of legitimate public concern must not be discouraged, *inter alia* by measures that make access to information more cumbersome or by arbitrary restrictions, which may become a form of indirect censorship.

14. The media ecosystem is shaped by the interplay of legal, political, socio-cultural, economic, technological and other influences and its vitality is crucial for ensuring an enabling environment for freedom of expression and information in democratic society. One feature of the media ecosystem is that individuals have become empowered as a result of new technologies that facilitate their ability to participate in public debate. Another feature of the media ecosystem is that online intermediaries may carry out an influential gate-keeping function in respect of public debate that is conducted via their private networks, such as social media. It must be recalled that online intermediaries are indirectly bound to respect their users' right to freedom of expression and other human rights.

15. Media pluralism and diversity of media content are essential for the functioning of a democratic society and are the corollaries of the fundamental right to freedom of expression and information as guaranteed by Article 10 ECHR. States have a positive obligation to guarantee pluralism in the media sector, which entails ensuring that a diversity of voices, including critical ones, can be heard. Independent media regulatory authorities can play an important role in upholding media freedom and pluralism and as such, states should safeguard their independence. The adoption and effective implementation of media-ownership regulation also plays an important role in this respect. Such regulation should ensure transparency in media ownership and prevent concentration of media ownership where it is detrimental to pluralism; it should address issues such as cross-media ownership, indirect media ownership and appropriate restrictions on media ownership by persons holding public office.

16. In the course of their work, journalists and other media actors often face specific risks, dangers and discrimination on grounds of their gender, gender identity, sexual orientation, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status. Moreover, the pursuit of particular stories and coverage of particular issues (such as sensitive political, religious, economic or societal topics, including misuse of power, corruption and criminal activities) can also expose journalists and other media actors to threats, attacks, abuse and harassment by State and/or non-State actors. Such non-State actors could, for instance, be terrorist or criminal groups. These specific situations should be taken into account when affording effective preventive or protective measures.

17. Female journalists and other female media actors face specific gender-related dangers in the course of their work, such as threats, (sexual) aggression and violence, in targeted ways, in the context of mob-related sexual violence, or sexual abuse while in detention. These dangers are often compounded due to various factors, such as under-reporting, under-documentation, lack of access to justice, social barriers and constraints concerning gender-based violence, including stigmatisation, lack of recognition of the seriousness of the problem

and discriminatory attitudes by extremist sections of society. A systematic, gender-sensitive approach is required to prevent and combat these specific dangers, as well as to counter the underlying societal customs, practices, gender stereotypes, prejudices and discrimination on which they feed. Primary responsibility for developing such strategies lies with state authorities, but media, civil society and corporate organisations also have important roles to play: a gender-specific perspective should be a central feature of all measures and programmes dealing with the protection of journalists and other media actors and the fight against impunity.

18. The ability to exercise the right to freedom of expression without fear implies that, as a minimum, the safety, security and protection of everyone, in particular journalists and other media actors, are guaranteed effectively in practice, and that there is an expectation that they can contribute to public debate without fear and without having to modify their conduct due to fear. Fear can arise from online harassment, threats and cyberattacks and other illegal behaviour, including trolling, cyberstalking, hacking of e-mail and social media accounts, storage, websites, as well as mobile phones and other electronic devices. Online harassment, threats, abuse and violations of digital security tend to target female journalists and other female media actors in particular, which calls for gender-specific responses. Threats and violence are not the only sources of fear, however. Fear can also be generated by (the threat or reasonable expectation of) a range of legal, political, socio-cultural and economic pressures, which can be exacerbated in times of economic crisis and financial austerity.

19. Threats to, and intimidation of, journalists and other media actors can often be seen as indicators or warning signals of wider or escalating threats to freedom of expression in society. As such, they point to a more general deterioration in human rights, democracy and rule of law.

Safety, Security, Protection

20. The State must guarantee the safety and physical integrity of everyone within its jurisdiction and this entails not only the negative obligation to refrain from the intentional and unlawful taking of life, but also the positive obligation to take appropriate steps to safeguard the lives of those within its jurisdiction. This positive obligation has substantive and procedural dimensions.

21. The substantive dimension involves a primary obligation for the State to secure the right to life by putting in place effective criminal-law provisions to deter the commission of offences against the person, backed up by law enforcement machinery for the prevention, suppression and punishment of breaches of such provisions. This also extends, in appropriate circumstances, to a positive obligation on the authorities to take preventive operational measures to protect an individual or individuals whose lives are at risk from the criminal acts of another individual. Bearing in mind the difficulties in policing modern societies, the unpredictability of human conduct and the operational choices which must be made in terms of priorities and resources, the scope of the positive obligation must be interpreted in a way which does not impose an impossible or disproportionate burden on the authorities. Nevertheless, the authorities should pay attention to the vulnerable position in which a journalist who covers politically sensitive topics places himself/herself *vis-à-vis* those in power.

22. Unregulated and arbitrary action by State agents is incompatible with effective respect for human rights. This means that, as well as being authorised under national law, policing operations, including the policing of public demonstrations, must be sufficiently regulated by it, within the framework of a system of adequate and effective safeguards against arbitrariness and abuse of force, and even against avoidable accident. This implies a need to take into consideration not only the actions of the agents of the State who actually administer the force but also all the surrounding circumstances, including such matters as the planning and control of the actions under examination. A legal and administrative framework should define the limited circumstances in which law-enforcement officials may use force and firearms, in the light of the international standards which have been developed on this topic. In this respect, a clear chain of command, coupled with clear guidelines and criteria are required; specific

human-rights training can help to formulate such guidelines and criteria. In any case, the undeniable difficulties inherent in the fight against crime cannot justify placing limits on the protection to be afforded in respect of the physical integrity of individuals and Article 3 ECHR does not allow for a balancing exercise to be performed between the physical integrity of an individual and the aim of maintaining public order.

23. The procedural dimension involves, first, a positive obligation on the state to carry out effective, independent and prompt investigations into alleged unlawful killings or ill-treatment, either by State or non-State actors, with a view to prosecuting the perpetrators of such crimes and bringing them to justice. Article 13 ECHR also requires states to ensure that an effective remedy is available whenever any of the Convention's substantive rights are violated.

24. The absence of such effective measures gives rise to the existence of a culture of impunity, which leads to the toleration of abuses and crimes against journalists and other media actors. When there is little or no prospect of prosecution, perpetrators of such abuses and crimes do not fear punishment. This inflicts additional suffering on victims and can lead to the repetition of abuses and crimes.

25. The State has an obligation to guarantee the substantive liberty of everyone within its jurisdiction and to that end must ensure that journalists and other media actors are not subjected to arbitrary arrest, unlawful detention or enforced disappearance.

26. The State should not unduly restrict the free movement of journalists and other media actors, including cross-border movement and access to particular areas, conflict zones, sites and forums, as appropriate, due to the importance of such mobility and access for news and information-gathering purposes.

27. The effectiveness of a system of protection may be influenced by contextual factors, such as in crisis or conflict situations, where there are heightened risks for the safety and independence of journalists and other media actors, and where state authorities may experience difficulties in exerting *de facto* control over the territory. Nevertheless, the relevant state obligations apply *mutatis mutandis* in such specific contexts, which are at all times subject to international human rights law and international humanitarian law.

28. Ensuring the safety and security of journalists and other media actors is a precondition for ensuring their ability to participate effectively in public debate. The persistence of intimidation, threats and violence against journalists and other media actors, coupled with the failure to bring to justice the perpetrators of such offences, engender fear and have a chilling effect on freedom of expression and on public debate. States are under a positive obligation to protect journalists and other media actors against intimidation, threats and violence irrespective of their source, whether governmental, judicial, religious, economic or criminal.

Contribution to public debate

29. Journalists and other media actors make an essential contribution to public debate and opinion-making processes in democratic society by acting as public or social watchdogs and by creating shared spaces for the exchange of information and ideas and for discursive interaction. The watchdog role involves, *inter alia*, informing the public about matters of public interest, commenting on them, holding public authorities and other powerful forces in society to account, exposing corruption and abuse of power.

30. In order to enable journalists and other media actors to fulfil the tasks ascribed to them in democratic society, the European Court of Human Rights has recognised that their right to freedom of expression should enjoy a broad scope of protection. Such protection includes a range of freedoms that are of functional relevance to the pursuit of their activities, such as: protection of confidential sources; protection against searches of professional workplaces and private domiciles and the seizure of materials; protection of news and information-gathering processes; editorial and presentational autonomy.

31. The operational or functionally-relevant freedoms enjoyed by journalists and other media actors, which cover news and information-gathering, processing and dissemination activities, are necessary for their right to freedom of expression to be practical and effective, both offline and online.

32. Article 10 ECHR protects not only the substance of the ideas and information expressed, but also the form in which they are conveyed. This implies that journalists and other media actors have the freedom to choose their own technique or style for reporting on matters of public interest, which includes possible recourse to a degree of exaggeration, or even provocation. Besides reporting, other genres also contribute to public debate in different ways and should accordingly be protected, like satire which is a form of artistic expression and social commentary and, by its inherent features of exaggeration and distortion of reality, naturally aims to provoke and agitate.

Chilling effect

33. A chilling effect on freedom of expression arises when an interference with the right causes fear, leading to self-censorship and ultimately the impoverishment of public debate, which is to the detriment of society as a whole. Accordingly, states' authorities ought to avoid taking measures or imposing sanctions that have the effect of discouraging participation in public debate.

34. Legislation and how it is applied in practice can give rise to a chilling effect on freedom of expression and public debate. Interferences that take the form of criminal sanctions have a greater chilling effect than those constituting civil sanctions. Thus, the dominant position of the State institutions requires the authorities to show restraint in resorting to criminal proceedings. A chilling effect on freedom of expression can arise not only from a disproportionate sanction or any sanction, but also the fear of sanction, even in the event of an eventual acquittal, considering the likelihood of such fear discouraging one from making similar statements in the future.

35. Although sentencing is in principle a matter for the national courts, the imposition of a prison sentence for a press offence will be compatible with journalists' freedom of expression as guaranteed by Article 10 ECHR only in exceptional circumstances, notably where other fundamental rights have been seriously impaired, as, for example, in the case of hate speech or incitement to violence.

36. Actual (mis-)use, abuse or threatened use of different types of legislation to prevent contributions to public debate, including defamation, anti-terrorism, national security, public order, hate speech, blasphemy and memory laws can prove effective means of intimidating and silencing journalists and other media actors reporting on matters of public interest. The frivolous, vexatious or malicious use of the law and legal process, with the high legal costs required to fight such law suits, can become a means of pressure and harassment, especially in the context of multiple law suits. The harassment can prove particularly acute when it concerns journalists and other media actors who do not benefit from the same legal protection or financial and institutional back-up as those offered by large media organisations. In this respect, it ought to be recalled that it is central to the concept of a fair trial, in civil as in criminal proceedings, that a litigant is not denied the opportunity to present his or her case effectively before the court and that he or she is able to enjoy equality of arms with the opposing side. States are required to take appropriate measures, which could include the institution of a legal aid scheme, in order to ensure that each side is afforded a reasonable opportunity to present his or her case under conditions that do not place him or her at a substantial disadvantage vis-à-vis the adversary.

37. A chilling effect also results from the (mis-)use of administrative measures such as registration and accreditation schemes for journalists, bloggers, internet users, foreign correspondents, NGOs, etc., and tax schemes, in order to harass journalists and other media actors, or to frustrate their ability to contribute effectively to public debate. The discriminatory allocation of public media or press subsidies or of state advertising revenue can also give rise

to a chilling effect on critical editorial lines pursued by the media, in particular for smaller media organisations and in precarious economic climates.

38. Practices of surveillance of journalists and other media actors, and the tracking of their online activities, can endanger the legitimate exercise of freedom of expression if carried out without the necessary safeguards. They can also threaten the safety of the persons concerned and undermine the protection of journalists' sources. Surveillance and tracking are facilitated when the integrity of communications and systems are compromised, for example, when service providers or hardware or software manufacturers build surveillance capabilities or backdoors into their services or systems, or when service providers are implicated in State surveillance practices. In order for systems of secret surveillance to be compatible with Article 8 ECHR, they must contain adequate and effective safeguards against abuse, including independent supervision, since such systems designed to protect national security entail the risk of undermining or even destroying democracy on the ground of defending it.

39. Attacks on, and intimidation of, journalists and other media actors inevitably have a grave chilling effect on freedom of expression and the chilling effect is all the more piercing when the prevalence of attacks and intimidation is compounded by a culture of legal impunity for their perpetrators. Such a culture of legal impunity is an indicator of endemic abuse of human rights.

APPENDIX IV

Draft Recommendation CM/Rec(2015)__ of the Committee of Ministers to member states on Internet freedom

(adopted by the Committee of Ministers on _____ 2015 at the __th meeting of the Ministers' Deputies)

1. The European Convention on Human Rights (hereinafter the ECHR) applies both offline and online. The Council of Europe member States have negative and positive obligations to respect, protect and promote human rights and fundamental freedoms on the Internet.

2. Internet freedom is understood as the exercise and enjoyment on the Internet of human rights and fundamental freedoms and their protection in compliance with the ECHR and the International Covenant on Civil and Political Rights. The member States of the Council of Europe should take a proactive approach to implement the ECHR and other Council of Europe standards with regard to the Internet. The understanding of Internet freedom should be a comprehensive one and firmly grounded on these standards.

3. Internet governance arrangements, whether national, regional or global, must build on this understanding of Internet freedom. States have rights and responsibilities with regard to international Internet-related policy. In the exercise of their sovereignty rights, States must, subject to international law, refrain from any action that would directly or indirectly harm persons or entities inside and outside of their jurisdiction. Any national decision or action restricting human rights and fundamental rights on the Internet must comply with international obligations and in particular be based on law, be necessary in a democratic society, fully respect the principles of proportionality and guarantee access to remedies and the right to be heard and appeal with due process safeguards.

4. As part of their obligation to secure to everyone within their jurisdiction the rights and freedoms enshrined in the ECHR, States should create an enabling environment for Internet freedom. To this end it is recommended that States carry out regular evaluations of the Internet freedom landscape at the national level with a view to ensuring that the necessary legal, economic and political conditions are in place for Internet freedom to exist and develop. Such evaluations contribute to a better understanding of the application of the ECHR to the Internet in member States and to its better implementation by national authorities.

5. The ECHR and Council of Europe standards provide benchmarks and references for national evaluations of Internet freedom. They can be considered as indicators which guide and enable member States to identify existing or potential challenges to Internet freedom, as an analytical framework to evaluate the implementation of human rights standards on the Internet and as a reference for developing international policy and approaches relating to the Internet.

6. The Council of Europe should play a key role in promoting Internet freedom in Europe and globally. Building on member States' national evaluations, the Council of Europe can observe the evolution of regulatory frameworks and other developments in its member States and provide regular overviews on the challenges to Internet freedom in Europe. This would be a good basis for further development of Council of Europe Internet-related policies.

7. The Committee of Ministers recommends that member States:

- periodically evaluate the respect and implementation of human rights and fundamental freedom standards with regard to the Internet using the indicators included in this recommendation, with a view to elaborating national reports, wherever appropriate;

- ensure the participation of all stakeholders from private sector, civil society, academia and the technical community in their respective roles in the evaluation of the state of Internet freedom and development of national reports;

- consider sharing on a voluntary basis information or national reports on Internet freedom with the Council of Europe;

- be guided by and promote these indicators when participating in international dialogue and international policy-making on Internet freedom;

- take appropriate measures to promote the United Nations "Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect, and Remedy" Framework.

8. The Committee of Ministers also invites the Secretary General of the Council of Europe to reflect on issues related to Internet freedom in his annual report on the state of democracy, human rights and the rule of law in Europe, with a special emphasis on the sharing of best practices. Such reflection should build also on national evaluations of member States.

INTERNET FREEDOM INDICATORS

Internet freedom is understood as the exercise and enjoyment on the Internet of human rights and fundamental freedoms and their protection in compliance with the ECHR. These indicators focus on the right to freedom of expression, the right to freedom of assembly and association, the right to private life and the right to an effective remedy. They build on the existing and established human rights standards and enforcement mechanisms. A comprehensive approach to Internet freedom considers all indicators. They are intended to provide guidance in conducting a qualitative and objective evaluation of and reporting on Internet freedom in Council of Europe member States. They are not designed to rate the levels of Internet freedom or as a means of comparing countries.

1. An enabling environment for Internet freedom

1.1. The protection of human rights and fundamental freedoms on the Internet is guaranteed in law in full compliance with the ECHR.

1.2. State interference with the exercise of human rights and fundamental freedoms on the Internet complies with the ECHR.

1.3. Laws and policies relating to the Internet are assessed at the stage of their development with regard to impact that their implementation may have on the exercise of human rights and fundamental freedoms.

1.4. Laws and policies relating to the Internet are developed by State authorities in an inclusive and transparent process which enables the participation of all stakeholders, including the private sector, civil society, academia and the technical community.

1.5. Any state body which has regulatory or other competence over Internet matters carries out its activities free from political or commercial interference, in a transparent manner and protects and promotes Internet freedom.

1.6. The State protects individuals from cybercrime through effective criminal justice or other measures. Where such measures risk interference with the right to private life, the right to freedom of expression or the right to freedom of peaceful assembly and association they are subject to conditions and safeguards against abuse. These measures comply with Articles 8, 10 and 11 of the ECHR, notably they are prescribed by law, which is precise, clear, accessible and foreseeable, pursue a legitimate aim, are necessary and proportionate in a democratic society and allow for effective remedies.

1.7. The State develops policies and takes measures to implement the United Nations "Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect, and Remedy" Framework".

1.8. The State provides media and digital literacy programmes for users to foster their ability to make informed decisions and to respect the rights and freedoms of others. The state promotes access to and use of educational, cultural, scientific, scholarly and other content.

2. The right to freedom of expression

2.1. Freedom to access the Internet

2.1.1. The Internet is available, accessible and affordable to all groups of population without any discrimination.

2.1.2. The public has access to the Internet in facilities supported by public administration (Internet access points), educational institutions or private owners (universal community service).

2.1.3. The State takes reasonable measures to ensure access to the Internet to those with low income, in rural or geographically remote areas and those with special needs such as persons with disabilities.

2.1.4. There are no general nation-wide restrictions on access to the Internet except when this is in compliance with Article 10 of the ECHR.

2.1.5. The State recognises in law and in practice that disconnection of individuals from Internet, as a general rule represents a disproportionate restriction of the right to freedom of expression.

2.1.6. Any restriction of Internet access, including in penitentiary institutions, complies with the conditions of Article 10 of the ECHR regarding the legality, legitimacy and proportionality of restrictions with freedom of expression and the positive obligation of the State to protect the right to freedom of expression.

2.1.7. Before Internet access restrictive measures are applied, a court or independent administrative authority determines that disconnection from Internet is the least restrictive measure for achieving the legitimate aim. The continuing necessity of the restrictive measure is evaluated by these authorities on a continuing basis. These conditions do not apply to cases of non-payment by users for their Internet services.

2.1.8. When restrictive measures are applied, the person concerned has the right to due process before a court or an independent administrative authority whose decisions are subject to judicial review, including the right to be heard and the right of appeal in compliance with Article 6 of the ECHR.

2.2. Freedom of opinion and the right to receive and impart information

2.2.1. Any measure taken by State authorities or private sector actors to block or otherwise restrict access to an entire Internet platform (social media, social networks, blogging or any other website) or ICTs tools (instant messaging or other applications) or request by State authorities to carry out such actions, complies with the conditions of Article 10 of the ECHR regarding the legality, legitimacy and proportionality of restrictions.

2.2.2. Any measure taken by State authorities or private sector actors to block, filter or remove Internet content, or any request by State authorities to carry out such actions complies with the conditions of Article 10 of the ECHR regarding the legality, legitimacy and proportionality of restrictions.

2.2.3. Internet service providers as a general rule treat Internet traffic equally and without discrimination on the basis of sender, receiver, content, application, service or device.

Internet traffic management measures are transparent, necessary and proportionate to achieve overriding public interests in compliance with Article 10 of the ECHR.

2.2.4. Internet users or other interested parties have access to an appeal procedure compliant with Article 6 of the ECHR with regard to any action taken to restrict their access to the Internet or their ability to receive and impart content or information.

2.2.5. The State provides information in a timely and appropriate manner to the public about restrictions it applies to the freedom to receive and impart information, such as explanation at the website which was blocked or from which information was removed, including details of the legal basis, necessity and justification for such restrictions, the court order authorising them and the right to appeal.

2.3. Freedom of the media

2.3.1. The editorial independence of media operating on the Internet is guaranteed in law/ policy and in practice. They are not subjected to pressure to include or exclude information from their reporting or to follow a particular editorial direction.

2.3.2. Media are not required to obtain permission or a licence from the government or state authorities which goes beyond business registration in order to be allowed to operate on the Internet or blog.

2.3.3. Journalists and other media actors using the Internet are not subject to threats or harassment by the State. They do not practice self-censorship because of fear of punishment, harassment or attack.

2.3.4. The confidentiality of journalists and other media actors' sources is protected in law and respected in practice.

2.3.5. Media websites as well as websites of new media actors are not affected by cyber-attacks or other action disrupting their functioning (e.g. denial of service attacks).

2.3.6. There are prompt and effective investigations of threats and crimes against journalists and new media actors. There is no climate of impunity.

2.4. Legality, legitimacy and proportionality of restrictions

2.4.1. Any restriction of the right to freedom of expression on the Internet is in compliance with the requirements of Article 10 of the ECHR, as interpreted by the ECtHR, namely:

- is prescribed by law, which is accessible, clear, unambiguous and sufficiently precise to enable individuals to regulate their conduct. The law ensures tight control over the scope of the restriction and effective judicial review to prevent any abuse of power. The law indicates with sufficient clarity the scope of discretion conferred on public authorities with regard to the implementation of restrictions and the manner of exercise of this discretion.

- pursues a legitimate aim as exhaustively enumerated in Article 10 of the ECHR;

- is necessary in a democratic society and proportionate to the legitimate aim. There is a pressing social need for the restriction, which is taken on the basis of a decision by a court or an independent administrative body that is subject to judicial review. The decision should be targeted and specific. Also, it should be based on an assessment of the effectiveness of the restriction and risks of over-blocking. This assessment should determine whether the restriction may lead to disproportionate banning of access to Internet content or to specific types of content and whether it is the least restrictive means available to achieve the stated legitimate aim.

2.4.2. The State does not impose undue restrictions to freedom of expression on the Internet by means of law. Defamation laws are specific and narrowly defined as to their scope of application. They do not inhibit public debate or criticism of State bodies and do not impose excessive fines or disproportionate awards of damages or legal costs. Severe sanctions, such as imprisonment, are applied only when the fundamental rights of other people have been seriously impaired such as in cases of incitement to violence or hatred.

2.4.3. Laws addressing hate speech or protecting public order, public morals, minors, national security or official secrecy and data protection laws are not applied in a manner which inhibits public debate. Such laws impose restrictions of freedom of expression only in response to a pressing matter of public interest, are defined as narrowly as possible to meet the public interest and include proportionate sanctions.

3. The right to freedom of peaceful assembly and association

3.1. Individuals are free to use Internet platforms, such as social media and other ICTs in order to associate with each other and to establish associations, to determine the objectives of such associations, to form trade unions, and to carry out activities within the limits provided for by laws that comply with international standards.

3.2. Associations are free to use the Internet in order to exercise their right to freedom of expression and to participate in matters of political and public debate.

3.3. Individuals are free to use Internet platforms, such as social media and other ICTs in order to organise themselves for purposes of peaceful assembly.

3.3. State measures applied in the context of the exercise of the right to peaceful assembly which amount to a blocking or restriction of Internet platforms, such as social media and other ICTs, comply with Article 11 of the ECHR.

3.4. Any restriction on the exercise of the right to freedom of peaceful assembly and right to freedom of association with regard to the Internet is in compliance with Article 11 of the ECHR, namely:

- is prescribed by law, which is accessible, clear, unambiguous and sufficiently precise to enable individuals to regulate their conduct;

- pursues a legitimate aim as exhaustively enumerated in Article 11 ECHR;

- is necessary in a democratic society and proportionate to the legitimate aim. There is a pressing social need for the restriction. There is a fair balance between the exercise of the right to freedom of assembly and freedom of association and the interests of the society as a whole. If a less intrusive measure is capable of achieving the same goal the least restrictive measure is applied. The restriction is narrowly construed and applied and does not encroach on the essence of the right to freedom of assembly and association.

4. The right to private and family life

4.1. Personal data protection

4.1.1. The right to private and family life is guaranteed in compliance with Article 8 of the ECHR as interpreted by the ECtHR. Any restriction to this right pursues one of the legitimate aims exhaustively enumerated in Article 8 of the ECHR, is necessary in a democratic society and proportionate to the legitimate aim pursued.

4.1.2. The law guarantees that all personal data is protected in compliance with Article 8 of the ECHR as interpreted by the ECtHR and the Convention for the Protection of

Individuals with regard to Automatic Processing of Personal Data (Convention 108) in States which have ratified it.

4.1.3. Personal data are processed lawfully (with the unambiguous consent of the data subject or on the basis of law) for legitimate purposes and not in excess of such purposes, accurately and securely. These conditions apply also to profiling (personal data automatic processing techniques that collect and use information about an individual in order to identify, analyse or predict his or her personal preferences, behaviour and attitudes).

4.1.4. Individuals are not subjected to a decision significantly affecting them based solely on automated processing of data without having their views taken into account. There are effective processes for every individual to obtain, on request, information on the processing of his or her personal data, the reason underlying processing; to object to processing; to obtain, on request, rectification or erasure of the personal data; and to consent to, object to or withdraw consent to personal data processing or profiling. Individuals have an effective remedy if these rights are not complied with. There are adequate safeguards for access to information and freedom of expression in the context of application of personal data protection legal frameworks.

4.1.5. The law defines the duties of public and private entities with regard to processing of personal data.

4.1.6. A supervisory authority, which acts with complete independence and impartiality, ensures compliance with data protection legal frameworks.

4.1.7. The State does not prohibit in law and in practice anonymity, pseudonymity and confidentiality of private communications or the usage of encryption technologies. Interference with anonymity and confidentiality of communications is subject to the requirements of legality, legitimacy and proportionality of Article 8 of the ECHR.

4.2. Surveillance

4.2.1. Surveillance measures taken by public authorities (such as security services) comply with the requirements of Article 8 the ECHR and are subject to effective, independent and impartial oversight.

4.2.2. Surveillance measures are carried out in accordance with the law, which is accessible, clear, precise and foreseeable. The law contains safeguards for the exercise of discretion by public authorities and thus defines with sufficient clarity and precision:

- the nature of offences which may give rise to surveillance measures;
- the competent authorities by which surveillance measures are carried out, the scope of any discretion conferred on such authorities and the manner of its exercise having regard to the legitimate aim of the measure in question;
- the categories of individuals liable to be subjected to surveillance measures;
- time limitations for carrying out surveillance measures;
- the procedures for examining, using and storing data obtained from surveillance measures;
- the precautions to be taken when communicating data acquired through surveillance measures to other parties and the measures applicable during the communication to ensure data security;
- the circumstances for the destruction and erasure of data obtained from surveillance measures;

- the bodies responsible for overseeing surveillance measures.

4.2.3. Surveillance measures pursue a legitimate aim as exhaustively enumerated in Article 8 of the ECHR, are necessary in a democratic society and proportionate to the legitimate aim pursued.

4.2.4. Surveillance measures carried out by State authorities either directly or through/in collaboration with private sector entities are authorised by an independent and impartial tribunal established by law or another State body who is independent from the authorities carrying out such measures and the executive.

4.2.5. Surveillance measures carried out by State authorities either directly or through/in collaboration with private sector entities do not involve activities which weaken encryption systems and the integrity of communications' infrastructure (for example built-in flaws and backdoors in security, information and communications systems).

4.2.6. Surveillance measures are subject to an effective review assured by a judicial authority or oversight by another state body offering the best guarantees of impartiality and independence from the authorities carrying out surveillance or the executive.

4.2.7. The law guarantees the right of an oversight body to have access to all information which is relevant to the fulfilment of its mandate, regardless of the level of information classification. Access to information by an oversight body extends to all relevant information held by public authorities including information provided by foreign bodies.

4.2.8. Oversight bodies exercise their powers, including seeking and handling classified information and personal data, professionally and strictly for the purposes for which they are conferred by law while ensuring that the information is protected from being used or disclosed for any purpose that is outside the mandate of such bodies.

4.2.9. Oversight bodies scrutinise, within their competences, the human rights compliance of surveillance measures taken by public authorities, including those taken in co-operation with foreign bodies through exchange of information or joint operations.

4.2.10. Judicial authorities and oversight bodies have the power to quash and discontinue surveillance measures undertaken when such measures are deemed to have been unlawful, as well as the power to require the deletion of any information obtained from the use of such measures.

4.2.11. Public authorities which carry out surveillance measures and their oversight bodies are not exempt from the ambit of freedom of information legislation. Decisions not to provide information are taken on a case-by-case basis, properly justified and subject to the supervision of an independent information/data commissioner. Oversight bodies make public informative versions of their periodic and investigation reports.

5. Remedies

5.1. The State ensures that individuals have access to judicial or administrative procedures that can impartially decide on their claims concerning violations of human rights online in compliance with Article 6 of the ECHR.

5.2. The State provides for the right to an effective remedy in compliance with Article 13 of the ECHR. This includes effective non-judicial mechanisms, administrative or other means for seeking remedy such as through national human rights institutions. There are no legal, procedural, financial or other practical barriers that individuals encounter in seeking an effective remedy.

5.3. The State, as the primary entity responsible, takes appropriate steps to protect against human rights abuses with regard to the Internet by private sector actors and to ensure that those affected have access to an effective remedy.

5.4. The State implements policies and measures to promote that all private sector actors respect human rights with regard to the Internet throughout their operations, in particular by establishing effective complaint mechanisms to address early and to remedy directly grievances of individuals whose human rights and fundamental freedoms on the Internet may be adversely impacted. Such mechanisms are legitimate (enabling trust, accountable for the fair conduct of grievances processes), accessible (known by those concerned, without barriers to access) predictable (providing a clear and known procedure with an indicative time frame for each stage, and clarity of types of processes and outcome available and means of monitoring implementation) equitable (reasonable access to sources of information, advice and expertise necessary to engage in a complaint process) transparent (keeping parties informed about the progress of a complaint) and compatible with Article 13 of the ECHR.

Draft Explanatory memorandum to the draft Recommendation CM/Rec__ (2015) ___of the Committee of Ministers to member States on Internet Freedom

Background and the process

1. The Ministers of States participating in the Council of Europe Conference of Ministers responsible for media and information society, held in Belgrade, Serbia, on 7 and 8 November 2013 adopted a Resolution on Internet freedom. The Resolution invited the Council of Europe to further develop, in a multi-stakeholder approach, the notion of "Internet freedom" on the basis of standards adopted by the Committee of Ministers on Internet governance principles, network neutrality and the universality, integrity and openness of the Internet".

2. The Committee of Ministers approved the terms of reference of the Committee of experts on cross-border flow of Internet traffic and Internet freedom (MSI-INT) at its 1185th meeting, 20 November 2013 (CM(2013)131add final). Under its terms of reference the MSI-INT is expected to prepare and submit to the CDMSI a draft recommendation on Internet freedom. Subsequently the Committee of Ministers Decisions of the Committee of Ministers adopted at the 1187th meeting, 11-12 December 2013 instructed the Steering Committee on Media and Information Society (CDMSI) "to develop, in a multi-stakeholder approach, the notion of "Internet freedom" on the basis of standards adopted by the Committee of Ministers on Internet governance principles, network neutrality and the universality, integrity and openness of the Internet".

3. The MSI-INT held its first meeting on 17 and 18 March 2014, in Strasbourg. While noting the potential broad nature of the notion of Internet freedom, the MSI-INT agreed to focus its reflections on defining the notion and exploring it further in discussions with stakeholders as appropriate in the European Dialogue on Internet Governance (EuroDIG, 12-13 June 2014, Berlin) and the Internet Governance Forum (IGF, 2-5 September 2014, Istanbul).

4. Discussions at the second meeting the MSI-INT, which took place on 3 and 4 July 2014 in Strasbourg, highlighted that the added value of this instrument would be to recommend that member states consider Internet freedom in a comprehensive manner. The draft recommendation could be envisaged as a tool to guide policy-makers and to help member states evaluate the state of Internet Freedom as well as structure the debate internationally regarding Internet freedom. The MSI-INT agreed on a preliminary draft recommendation which aims at encouraging member State to implement human rights standards online and includes a list of indicators on Internet freedom.

5. At its working meeting, which took place on 23 and 24 October 2014 in Strasbourg, the MSI-INT validated the general approach taken in the draft recommendation as regards periodical reviews of the state of Internet freedom at a national level on the basis of the indicators set out in the draft recommendation. The objective is to promote an enabling environment in Council of Europe member states for the exercise and enjoyment of fundamental rights and freedoms online. The Internet freedom indicators should be geared towards facilitating an effective implementation of human rights standards. Participants from the private sector considered that the draft recommendation would be able to give guidance to civil society and citizens to strengthen their observatory role on Internet freedom. The CDMSI at its 7th meeting (18-21 November 2014) took note of the preliminary draft recommendation and invited its members to send possible comments to the MSI-INT.

6. At its third meeting, which took place on 5 and 6 March 2015 in Strasbourg, the MSI-INT discussed extensively the preamble and the operative parts of the draft recommendation. Pursuant to the Committee of Ministers Decision to develop in a multi-stakeholder approach the notion of Internet freedom, the MSI-INT agreed to organise multi-stakeholder consultations until the end of April 2015. Therefore, the MSI-INT agreed to propose to the Bureau of the CDMSI that the Steering Committee on Human Rights Policy (CDDH), the Steering Committee on Crime Problems (CDPC), the European Committee on Legal Cooperation, the Consultative Committee of the Data Protection Convention (T-PD) and the

Cybercrime Convention Committee (T-CY) be invited to provide their comments. In addition, the draft recommendation should be uploaded on the website of the Council of Europe and stakeholders be invited to comment.

7. Further to approval by the Bureau of the CDMSI of the MSI-INT proposals multi-stakeholder consultations were organised during the period of time 30 April – 14 May 2015. Comments were offered by members of the CDDH, CDCJ and the T-PD Bureau and TC-Y. In addition, around 30 contributions were received from representatives of the private sector (telecommunications companies, online service providers), key civil society organisations, the technical community as well as academicians from different parts of the world. They generally welcomed the Council of Europe's work on the draft recommendation and provided numerous comments and proposals for changes thereto.

8. The CDMSI, at its 8th meeting (16-19 June 2015), took note of the comments provided during the multi-stakeholder consultations. It supported the overall strategic approach of the draft recommendation to promote implementation of existing human rights standards on the Internet. It agreed to invite delegations to provide comments to the MSI-INT by 31 July 2015.

9. The MSI-INT, at its last meeting (7-8 September 2015, Strasbourg), finalised its proposals to the CDMSI for a draft recommendation by the Committee of Ministers CM/Rec(2015)__ to the member States on Internet freedom.

10. The CDMSI at its 9th meeting (8-11 December 2015, Strasbourg) finalised a draft recommendation by the Committee of Ministers CM/Rec(2015)__ to the member States on Internet freedom and agreed to transmit it to the Committee of Ministers for possible adoption.

11. Commentary on Recommendation CM/Rec (2014)___ of the Committee of Ministers to member States on Internet freedom.

Preamble of the Recommendation

12. The preamble affirms the principle that human rights and fundamental freedoms apply both to offline and online environments. The key standard is the ECHR. The central idea of the preamble is that Internet freedom should not be considered as a matter of choice with regard to which rights and freedoms should be protected. Instead a comprehensive approach with regard to all indicators should be taken.

13. Internet freedom is understood as the exercise and enjoyment on the Internet of human rights and fundamental freedoms. States are the duty bearers with regard to the protection and promotion of human rights in compliance with the ECHR. The role and the participation of States in Internet governance arrangements is considered as one of the conditions for the realisation of human rights and fundamental freedoms. Hence, the recommendation makes reference in paragraph 3 to the role and responsibilities of States with regard to international Internet-related policy. This paragraph is based on the Declaration of Committee of Ministers on Internet governance principles adopted in 2011.

14. The recommendation is based on the premise that in order for Internet freedom to exist it is necessary that legal, economic and political conditions are in place. It is the role of States to evaluate whether such conditions exist. Consequently it is recommended that member States evaluate the Internet freedom landscape using the indicators identified on the basis of existing Council of Europe standards. These evaluations will help member States to evaluate the state of play with regard to the implementation of standards and will provide an impetus for better and more effective implementation whenever this is necessary. The ECHR and other Council of Europe standards provide benchmarks and references for national evaluations of Internet freedom. Therefore, they can be conceptualised as indicators of Internet freedom.

15. In the operative part of the recommendation the Committee of Ministers recommends to member States to periodically evaluate how human rights standards are implemented and respected. Member States are better placed to assess the frequency or periodicity of self-

assessment and preparation of Internet freedom report, based on their appreciation of their institutional capacities to prepare such reports. Also, it is left to the appreciation of member States whether or not they share national reports on Internet freedom with the Council of Europe. These reports can be considered as part of the reflection by the Secretary General in the preparation of his annual report on the state of democracy, human rights and rule of law in Europe. The objective is to promote the implementation of existing standards and the sharing of best practices.

Internet Freedom Indicators

16. The indicators included in the Recommendation are intended to provide guidance in conducting a qualitative and objective evaluation of and reporting on the enabling environment for Internet freedom in Council of Europe member states. The explanatory memorandum provides complementary information on their basis in international human rights standards. In addition, it suggests sources of verification wherever applicable to the indicators, which can be used by national authorities when completing national evaluations.

1. An enabling environment for Internet freedom

17. A key principle of the Council of Europe's Internet-related standards, that is fundamental rights and freedoms apply both to online and offline environments . The European Court of Human Rights (ECtHR) has affirmed that "the Internet has now become one of the principal means by which individuals exercise their right to freedom of expression and information, providing as it does essential tools for participation in activities and discussions concerning political issues and issues of general interest." The ECtHR has underscored that the Internet is an important medium where citizens exercise their fundamental rights and that ECHR rights apply to the Internet . The UN Special Rapporteur on freedom of expression stated that the Internet acts as a "catalyst for individuals to exercise their right to freedom of opinion and expression the Internet also enables the realisation of a range of other human rights".

18. *Indicator 1.1.* seeks to verify that the State has enshrined these principles in its legal system. This could be done in constitutional or other laws, addressing the issue of human rights protection. These would be the sources of verification in evaluations based on this indicator. This indicator does not require that constitutional or other laws specifically mention their application to the Internet. It is important that their application is not limited to the physical world only, thus excluding the implementation of human rights standards with regard to the Internet. Another form of verification could be any international human rights treaties accepted by member States with no significant exemptions or any other integration of international human rights standards in legislation or policy related to the Internet.

19. Member States should assess the compliance of their actions which interfere with the right to private life, the right to freedom of expression, and the right to freedom of assembly and association with Articles 8, 10 and 11 of the ECHR. Sources of verification of *Indicator 1.2.* are laws and policies that restrict these rights and freedoms. These should be in compliance with the requirements of the ECHR as interpreted by the ECtHR: any restrictions pursue one of the legitimate aims foreseen in the ECHR and are necessary and proportionate in a democratic society. The least restrictive means should be used to achieve the legitimate aim.

19. Further verification will be that States ensure that private actors are able to provide the guarantees for these rights and freedoms, where those actors are operating infrastructure or facilities necessary for their exercise. The United Nations Guiding Principles on Business and Human Rights provide additional guidance. The ECtHR has held States accountable for failing to protect their citizens from adverse effects on their rights and freedoms resulting from actions of private companies.

20. Regulation of Internet issues is often distributed in different legal or policy instruments. Hence it is necessary not only to coordinate their preparation for coherence but also to asses the negative impact they could have on the exercise and enjoyment of human rights and fundamental freedoms. In addition, such approach will enable States to establish a careful

balance of the competing rights. *Indicator 1.3.* asks States to assess how any such laws and policies restricting these rights and freedoms have been balanced against other rights and freedoms being protected and that the appropriate legal tests are conducted.

21. States also have a duty to ensure the foreseeability of any laws and policies that they put in place in compliance with the requirements and principles established by the ECtHR in interpretation of the ECHR. An element of foreseeability is that laws and policies are assessed for compliance with ECHR before they are adopted, and that such compliance requirement is fully respected by the State. Any report, supporting explanatory statement on draft legislation or policy can serve as a source of verification.

22. *Indicator 1.4*. is based on the principle of multi-stakeholder governance included in the Committee of Ministers Declaration on Internet Governance principles. It builds on the definition of Internet governance, this principle affirms the multi-stakeholder nature of Internet environments. It reflects the understanding of the Geneva Declaration of Principles which states that "[g]overnments, as well as private sector, civil society and the United Nations and other international organizations have an important role and responsibility in the development of the Information Society and, as appropriate, in decision-making processes. Building a people-centred Information Society is a joint effort which requires co-operation and partnership among all stakeholders." It also underlines that "[t]he international management of the Internet should be multilateral, transparent and democratic, with the full involvement of governments, the private sector, civil society and international organizations".

23. The requirement of foreseeability of laws means that individual citizens must be able to foresee the consequences of its application to him/her and the law must also be formulated with sufficient clarity and precision to give citizens an adequate indication of the conditions and circumstances in which the authorities are empowered to act. An open process of law making will assist with the foreseeability requirement.

24. As a means of verification of this indicator, use can be made of any information, such as reports, articles or otherwise, on activities undertaken by competent State authorities to consult with stakeholders. These activities can include conferences, meetings, seminars, public fora, consultations on draft laws and policies or any other form of engagement of public officials in public debates around Internet related policy issues.

25. *Indicator 1.5*. requires wherever the law provides that executive authorities or regulatory bodies have discretion to implement measures which restrict the exercise or enjoyment of fundamental rights and freedoms, the law provides sufficient safeguards for the autonomy and independence from political or commercial interests. The members of regulatory bodies should be chosen through a democratic and transparent process in order to minimize partisan or commercial interference. Their powers and responsibilities should be set out in law, including explicit requirements to promote freedom of expression, the free flow of information, privacy and freedom of assembly and association. Any law or other legal instrument on the role membership, and competencies of regulatory bodies can serve as means of verification of this indicator.

26. Internet users and individuals in general should be protected from cybercrime. This will create a secure environment in which all will feel safe to exercise their rights and freedoms, hence contributing to the overall environment for Internet freedom. Indicator 1.6. can be verified by any law or policy which criminalises offences against the confidentiality and integrity of computer data and systems; content related offences (child pornography, copyright infringement); illegal access to the whole or parts of computer systems (hardware, components, stored data etc.);intrusion into computer systems (hacking, cracking or other forms of computer tress pass) which may lead to access to confidential data; computer data interference, such as malicious code (for example viruses and Trojan horses); interference with the functioning of computer or telecommunication systems by inputting, transmitting, damaging deleting, altering or suppressing computer data as for example programmes that generate 'denial of service attacks, malicious codes such as viruses that prevent or substantially slow down the operation of the system, or programmes that send large quantities

of electronic mail to a recipient in order to block communication functions of the system (spamming); computer forgery etc. All measures taken to combat cybercrime should comply with the articles 8, 10 and 11 of the ECHR.

27. Since Internet companies are the main interlocutor or the party with which individuals have contacts with regard to the exercise of the human rights and freedoms on the Internet their responsibilities to protect, respect and remedy these rights are key to the creation of an enabling environment for Internet freedom to exist and develop. Therefore, Indicator 1.7. refers to the United Nations Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework. The Guiding Principles provide that states should enforce laws that are aimed at, or have the effect of, requiring business enterprises to respect human rights, and periodically to assess the adequacy of such laws and address any gaps; ensure that other laws and policies governing the creation and ongoing operation of business enterprises, such as corporate law, do not constrain but enable business respect for human rights; provide effective guidance to business enterprises on how to respect human rights throughout their operations; encourage, and where appropriate require, business enterprises to communicate how they address their human rights impacts.

28. A foundational principle of the Guiding Principles on Business and Human Rights is that business enterprises should respect human rights, which means that they should avoid infringing on the human rights of others and address adverse human rights impact with which they are involved. The transparency and accountability of private sector actors is emphasised as an important means of demonstrating their responsibility as is actively promoting and disseminating it.

29. The United Nations Guiding Principles on Business and Human Rights specify that companies should establish complaint mechanisms which are accessible, predictable (providing clear and known procedure with indication of time frames for each stage of the process, clarity on the types of process and outcomes available and the means for monitoring their implementation) equitable (access to sources of information, advice and expertise), transparent and capable to offer remedies which are in full compliance with international human rights standards directly to individuals.

30. *Verification of Indicator 1.7*. can be sought in any law and policy which implements the Guiding Principles explained above or any other action plan or strategic document to promote the protection of human rights and fundamental freedoms by business enterprises.

31. Internet freedom also comprises positive rights and freedoms such as the right to education, which is enshrined in Article 2 of Protocol 1 to the ECHR. Indicator 1.8. addresses the issue of digital literacy as an enabler to other freedoms, and also the general promotion of access to the Internet for the purpose of education and access to culture. Digital literacy means that citizens should have the ability to acquire basic information, education, knowledge and skills in order to exercise their human rights and fundamental freedoms on the Internet.

32. This is in line with the Council of Europe's Committee of Ministers standards which promote computer literacy as a fundamental prerequisite for access to information, the exercise of cultural rights and the right to education. The Recommendation CM/Rec(2007)16 of the Committee of Ministers to member States on measures to promote the public service value of the Internet encourages 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. Citizens should be able to freely access publicly funded research and cultural works on the Internet. Access to digital heritage materials, which are in the public domain, should also be freely accessible within reasonable restrictions. Conditions on access to knowledge are permitted in specific cases in order to remunerate right holders for their work, within the limits of permissible exceptions to intellectual property protection.

33. In addition, Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a guide to human rights for Internet users also provides explanations to Internet

users on their human rights and fundamental freedoms online as well as their responsibilities to respect the rights of others. Verification of Indicator 1.8. will be the existence of State-funded digital literacy programmes, and other programmes promoting access to culture and knowledge via the Internet. Further verification will be the implementation of Council of Europe's Guide to Human Rights for Internet Users.

2. The Right to Freedom of Expression

2.1. Freedom to access the Internet

34. The ECtHR has affirmed in its jurisprudence that Article 10 is fully applicable to the Internet since any restriction imposed on the latter necessarily interferes with the right to receive and impart information. Hence, access to infrastructure is a prerequisite and an enabler for the realisation of the objective to guarantee freedom of expression . In this context, the Council of Europe's Committee of Ministers has acknowledged that the protection of Internet infrastructure protection should be a priority. To ensure that all citizens have the ability to access the Internet, the state should implement infrastructure policies to make sure that the Internet is available, accessible and affordable to all groups of the population and promote the principle of universality of the Internet.

35. *Indicator 2.1.1*. is concerned with access to the Internet, and the means by which the subscriber is able to connect to it. It addresses the universal ability to access the Internet across all areas and regions of the State, irrespective of the technology used to provide that access. Positive action or measures taken by state authorities to ensure that everyone is connected to the Internet is another dimension of the issue of access to the Internet. Public service value of the Internet is understood as "people's significant reliance on the Internet as an essential tool for their everyday activities (communication, information, knowledge, commercial transactions) and the resulting legitimate expectation that Internet services be accessible and affordable, secure, reliable and ongoing."

36. Verification of this indicator would be established by positive action or measures taken by State authorities to ensure that all citizens are able to obtain an Internet connection, for example, laws or policies on universal access to the Internet, including geographic coverage of network infrastructure. Metrics could be provided by reports or studies of Internet accessibility and infrastructure coverage, or through analysis of initiatives, programmes or investments in Internet infrastructure.

37. *Indicator 2.1.2*. is based on Council of Europe Recommendation CM/Rec (2007)16 of the Committee of Ministers to member states on measures to promote the public service value of the Internet. Public authorities should make reasonable efforts to facilitate access to the Internet for specific categories of individuals such as those living in remote areas and people with disabilities. This is based on the principle of universal community service which is laid down in Recommendation No.R(99)14 of the Committee of Ministers concerning new communication and information services. It emphasises that individuals living in rural or geographically remote areas or those with low income or special needs or disabilities can expect specific measures from public authorities in relation to their Internet access.

38. *Indicator 2.1.3* is based on the principle of universal community service which is laid down in Recommendation No.R(99)14 of the Committee of Ministers concerning new communication and information services. It emphasises that individuals living in rural or geographically remote areas or those with low income or special needs or disabilities can expect specific measures from public authorities in relation to their Internet access. The State should make reasonable efforts to facilitate access to the Internet for specific categories of individuals such as those living in remote areas and people with disabilities. This indicator is also based on the principle of non-discrimination as enshrined in article 14 of the ECHR.

39. This indicator seeks to verify the efforts made by the State to ensure that Internet access is made available to vulnerable individuals, such as the disabled, and to minority groups. Metrics could be provided by reports on Internet accessibility, notably initiatives or

programmes in support of access to the Internet for persons with disabilities and linguistic minorities.

40. *Indicator 2.1.4* is based on the jurisprudence of the ECtHR, in particular as regards the requirements on the rule of law and proportionality of measures taken by State authorities which interfere with the right to freedom of expression. When such measures are taken it is necessary that legal framework is in place which ensures both tight control over the scope of bans and effective judicial review to prevent any abuse of power. The legal framework should also include an obligation that courts assess the proportionality of measures. An effective judicial review involves also an assessment whether other less restrictive measures were possible. A blanket prohibition of access to the Internet, as for instance a measure that makes networks unavailable or disrupts their functioning, is considered as incompatible with these requirements. This indicator is also concerned with the possibility that access to the infrastructure is not available on a blanket basis within a given geographic area or to a group of the population.

41. Positive verification that the requirements of this indicator are met would be provided by any law that explicitly forbids blanket prohibitions on Internet access. Transparency reports on network availability from regulators, Internet service providers or non-governmental bodies would provide additional verification. Negative verification would be provided by any evidence or technical report that the Internet access is prohibited or regularly unavailable for the population of a country, or in specific regions or areas.

42. *Indicators 2.1.5 – 2.1.8*. specifically address the situation of disconnection of individuals from the Internet both in the context of implementation of a measures by the State or by an access provider. These indicators seek to verify that disconnections take place only if they are compatible with Article 10 of the ECHR. Measures which disconnect an individual from the Internet have a disproportionate impact on the right to access information and freedom of expression because they render large quantities of information inaccessible. Although access to the Internet is not yet formally recognised as a human right (noting differences in national contexts including domestic law and policy), it is considered as a condition and an enabler for freedom of expression and other rights and freedoms . Consequently, the disconnection of an Internet user could adversely affect the exercise of her/his rights and freedoms and could even amount to a violation of the right to freedom of expression, including the right to receive and impart information.

43. This, however, should not be understood as pre-empting legitimate disconnection measures such as in the context of obligations stemming from contractual obligations. Internet consumers who do not pay for their service may be disconnected from the Internet. This should, nonetheless, be a measure of last resort. Moreover, children can be subjected to discontinuation of access to the Internet in the context of exercise of parental control over Internet usage of the Internet, depending on the child's age and maturity. Also, the State may apply disconnection measures in penitentiary institutions ensuring compliance with Article 10 of the ECHR.

44. Every citizen, in the exercise of his right to fair trial, should be able to request a review of the disconnection measure by a competent administrative and/or judicial authority. If a situation arises where measures of disconnection from the Internet are not decided by a court, Internet users should have effective remedies against such measures, in compliance with Article 6 of the ECHR.

45. Verification of this indicator may be effected using reports by non-governmental organisations, such as those of Article 19, Center for Democracy & Technology , Electronic Frontier Foundation, or Freedom House.

3. 2. Freedom of opinion and the right to receive and impart information

46. *Indicators 2.2.1. and 2.2.2* addresses laws and policies of States with regard to content made available or distributed on Internet platforms and compliance with Article 10 of the

ECHR. In the Internet context, the right to receive and impart information, as referred to in Article 10 of the ECHR, applies to uploading (imparting) of content, as well as to downloading or viewing or otherwise accessing content, and the use of services, including anonymously. The Council of Europe's Committee of Ministers has affirmed that every Internet user should have the greatest possible access to Internet-based content, applications and services of his/her choice, whether or not they are offered free of charge, using suitable devices of his/her choice. Internet users should be free to express their political convictions as well as their religious and non-religious views.

47. The latter concerns the exercise of the right to freedom of thought, conscience and religion as enshrined in Article 9 of the ECHR. Freedom of expression is applicable not only to "information" or "ideas" that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb. The Court has affirmed that the effective exercise of the right to freedom of expression may also require positive measures of protection, even in the sphere of relations between individuals. The responsibility of the State may be engaged as a result of failing to enact appropriate domestic legislation.

48. Verification of this indicator would be established if laws or policies providing for restrictions on access to content, platforms and services on the Internet include specifically safeguards for the right to freedom of expression. In particular, this indicator is concerned with restrictions by means of, for example, blocking or filtering, which may be imposed via the Internet infrastructure using automated technologies (by Internet service providers or by other types of content or service providers). Verification can be assisted by reports from international human rights organisations such as those of the OSCE Representative on Freedom of the Media, the UN or the EU.

49. *Indicator 2.2.3.* seeks to verify that laws or policies provide sufficient safeguards against abusive restrictive measures, notably by defining clearly and precisely the scope of such measures and providing for effective control by a court or other independent adjudicatory body. It also addresses the proportionality of decisions taken by courts or independent administrative bodies regarding blocking, filtering or other restrictive measures. This indicator should be assessed in conjunction with those in section 2.4.

50. This indicator is based on the jurisprudence of the ECtHR, which has found that blocking or filtering of Internet access or content are examples of the kind of restrictions or interference which may engage freedom of expression. There should be strict control of the scope of blocking and effective judicial review to prevent any abuse of power. Judicial review of such a measure should weigh-up the competing interests at stake, strike a balance between them and determine whether there a less far-reaching measure could be taken to block access to specific Internet content. General principles with regard to blocking and filtering, based on the Court case law, have been incorporated into standards adopted by the Committee of Ministers.

51. States should ensure that all filters are assessed both before and during their implementation to ensure that their effects are proportionate to the purpose of the restriction and thus necessary in a democratic society, in order to avoid unjustified blocking of content . Measures taken to block specific Internet content must not be arbitrarily used as a means of general blocking of information on the Internet. They must not have a collateral effect in rendering large quantities of information inaccessible, thereby substantially restricting the rights of Internet users. They should be prescribed by law.

52. In this context, Internet restrictions such as blocking or filtering measures should specify clearly identifiable content, and should be based on a decision on the legality of the content by a competent national authority in accordance with the requirements of Article 6 of the ECHR. It should be possible for that decision to be reviewed by an independent and impartial tribunal or regulatory body. The requirements and principles mentioned above do not prevent the installation of filters for the protection of minors in specific places where minors access the Internet such as schools or libraries.

53. *Indicator 2.2.3*. seeks to assess the legal basis for the technological methods by which restrictions may be imposed on Internet content. The Committee of Ministers has emphasised that "users' right to access and distribute information online and the development of new tools and services might be adversely affected by non-transparent traffic management, content and services' discrimination or impeding connectivity of devices" . The Committee has emphasised its commitment to the principle of network neutrality, in order that users may have the greatest possible 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. Such a general principle, should apply with regard to all types of infrastructure or the network used for Internet connectivity.

54. Exceptions to this principle should be considered with great circumspection and need to be justified by overriding public interests. In this context, member States paying due attention to the provisions of Article 10 of the European Convention on Human Rights and the related case law of the European Court of Human Rights, may also find it useful to refer to the guidelines of 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.

55. Verification is possible in any law, regulation or policy that addresses the conditions for blocking and filtering Internet and Internet traffic management. Also, reports by regulatory authorities in the field of telecommunications can be sources of verification.

56. *Indicator 2.2.4.* addresses the requirement for compliance with ECHR Article 6, the right to due process, in instances where restrictions are applied to Internet content. States, as part of their positive obligations to protect individuals against violations of human rights by private companies, should take appropriate steps to ensure that when such violations occur, those affected have access to non-judicial mechanisms, in addition to judicial remedies. There must be a specific legal avenue available whereby individuals can address a complaint regarding restrictions of their rights, including the length of proceedings in the determination of their rights. This could be provided by a public authority, whose powers and the procedural guarantees would permit a determination whether a particular remedy is effective. That authority may not necessarily be a judicial authority, but it should present guarantees of independence and impartiality.

58. States should also ensure that private actors who are mandated to implement Internet restrictions establish complaint or appeal mechanisms. Those mechanisms should be accessible, predictable (providing clear and known procedure with indication of time frames for each stage of the process, clarity on the types of process and outcomes available and the means for monitoring their implementation) equitable (access to sources of information, advice and expertise), transparent and capable of offering remedies which are in full compliance with international human rights standards directly to individuals. The United Nations Guiding Principles on Business and Human Rights provide additional guidance.

59. *Indicator 2.2.5*. This indicator is concerned with the transparency of State action or measures with regard to any restrictions imposed. This is important for Internet users to be able to challenge such action or measures. States should focus on providing information to Internet users (both those who access information and those who disseminate it) and ensure that there are possibilities to challenge any restrictions imposed. Information should be given about when filtering has been activated, why a specific type of content has been filtered and to understand how, and according to which criteria, the filtering operates (for example black lists, white lists, keyword blocking, content rating, de-indexation or filtering of specific websites or content by search engines). There should be information about the manual overriding of an active filter, including contact information.

60. There should be clear and transparent information regarding the means of redress available. This information could be included in terms of use and/or service or in other guidelines and policies of Internet service/online providers. It should be possible to request information and seek remediation. There should be effective and readily accessible means of

recourse and remedy, including the suspension of filters; in cases where users claim that content has been blocked unjustifiably. It can be verified by means of the publicly available information regarding blocking as well as by using reports authored by non-governmental organisations such as Freedom House.

2.3. Freedom of the media

61. *Indicator 2.3.1.* is concerned with freedom of the media which is a corollary to freedom of expression. These freedoms are indispensable for genuine democracy and democratic processes. Editorial freedom or independence is an essential component of media freedom. States have a duty to guarantee that the media can publish independently without interference. This indicator seeks to establish that this guarantee is upheld in the online context, where the notion of what constitutes 'media' has evolved. In 2011, the Committee of Ministers adopted a new notion of media which encompasses all actors involved in the production and dissemination.

62. Verification of this indicator is possible if a law or policy exists that guarantees freedom of media and new media actors to produce, disseminate content and information without interference. Further sources of verification may be supplied by any report by civil society, independent organisations concerning documented cases of interference with editorial decision making, such as the OSCE reports on media freedom or Reporters Without Borders "Enemies of the Internet" reports or Index on Censorship media freedom reports and reports from Article 19 and Freedom House.

63. *Indicator 2.3.1.* seeks to verify that any licence or permission to operate as media actor on the Internet is related solely to the ability to set up in business and is not politically motivated.

64. It is based on the Recommendation of the Committee of Ministers to member States on a new notion of media, which recommends a "review of 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." This recommendation also states that "[s]ubject to the principle that, as a form of interference, media regulation should comply with the requirements of strict necessity and minimum intervention, specific regulatory frameworks should respond to the need to protect media from interference (recognising prerogatives, rights and privileges beyond general law, or providing a framework for their exercise), to manage scarce resources (to ensure media pluralism and diversity of content – cf. Article 10, paragraph 1 in fine, of the European Convention on Human Rights) or to address media responsibilities (within the strict boundaries set out in Article 10, paragraph 2, of the Convention and the related case law of the European Court of Human Rights)."

65. This indicator also finds basis in Resolution 1636 (2008) "Indicators for media in a democracy" of the Parliamentary Assembly of the Council of Europe which states that "regulatory authorities for the broadcasting media must function in an unbiased and effective manner, for instance when granting licenses. Print media and Internet-based media should not be required to hold a state license which goes beyond a mere business or tax registration".

66. In addition, the Committee of Ministers declared in 2011 that privately operated media platforms should be able to operate freely. Citizens rely on social networks, blogs, websites and online applications to access and exchange information, publish content, interact, communicate and associate with each other. These platforms are becoming an integral part of the new media ecosystem. Although privately operated, they are a significant part of the public sphere in that they facilitate debate on issues of public interest; in some cases, they can fulfil, similar to traditional media, the role of a social "watchdog" and have demonstrated their usefulness in bringing positive real-life change.

67. Verification may be provided by international media freedom reports, such as those from the Council of Europe's Commissioner for Human Rights, the OSCE , and the European Parliament report on Freedom of the Media in the Western Balkans as well as reports from Article 19, Freedom House, Index on Censorship and Reporters Without Borders.

68. *Indicator 2.3.3*. seeks to verify that the State does not interfere with journalists and others who perform public watchdog functions through online media. Obstacles created by the State in order to hinder access to information of public interest may not only discourage journalists and other new media actors from fulfilling a public watchdog role , but may also have negative effects on their safety and security as well as on their ability to inform the public. Attacks against journalists and other new media actors constitute particularly serious violations of human rights because they target not only individuals, but deprive others of their right to receive information, thus restricting public debate, which is at the very heart of pluralist democracy.

69. The ECtHR has held that the role played by journalists in a democratic society confers upon them certain increased protections under Article 10 of the ECHR. States have a duty to create a favourable environment for participation in public debate by all persons, enabling them to express their opinions and ideas without fear. To do this, States must not only refrain from interference with individuals' freedom of expression, but are also under a positive obligation to protect their right to freedom of expression against the threat of attack, including from private individuals, by putting in place an effective system of protection.

70. The Committee of Ministers has urged member States to fulfil their positive obligations to protect journalists and other media actors from any form of attack and to end impunity in compliance with the ECHR and in the light of the case law of the ECtHR. In this connection, it has also invited member States to review at least once every two years the conformity of domestic laws and practices with these obligations on the part of member States. Member States have also been encouraged to contribute to the concerted international efforts to enhance the protection of journalists and other media actors by ensuring that legal frameworks and law-enforcement practices are fully in accord with international human rights standards. The implementation of the UN Plan of Action on the Safety of Journalists and the Issue of Impunity is an urgent and vital necessity.

71. This indicator could be verified if there are either documented cases of online threats and harassment, or documented cases of investigations and prosecutions of journalists in relation to the exercise of their activity online, such as those cited in the regular reports by the OSCE special rapporteur for Media Freedom or Reporters Without Borders "Enemies of the Internet" reports.

72. *Indicator 2.3.4*. seeks to verify that the confidentiality of journalist's sources is protected and that they not are not subject to surveillance. Surveillance of journalists and other new media actors, and the tracking of their online activities, can endanger the legitimate exercise of freedom of expression on the Internet and can even threaten the safety of the persons concerned. It can undermine or expose their sources. In the Internet context, surveillance may entail the monitoring or storing of private communications, including the content, or gathering, storage and analysis of communications traffic data or metadata. Council of Europe's Committee of Ministers has provided guidance on these issues, notably in the Declaration of the Committee of Ministers on the protection of journalism and safety of journalists and other media actors and Recommendation Rec(200)7 on the right of journalists not to disclose their sources of information.

73. This indicator may be verified by the existence of any law or policy that guarantees the confidentiality of journalistic sources. Further verification may be found where documented cases exist of journalists' communications and work products being monitored, such as those cited by Reporters without Borders.

74. *Indicator 2.3.5*. addresses the possibility that free speech online is being challenged in new ways. For example, is based on the Committee of Ministers has expressed concern regarding

distributed denial-of-service attacks against websites of independent media, human rights defenders, dissidents, whistle-blowers and other new media actors. Such attacks represent interferences with the right to impart and receive information and with the right to freedom of association. They may have a negative effect on web-hosting services that may not wish to host sensitive content. This indicator may be verified by checking any reports concerning documented cases of denial of service attacks, hacking, defacement, phishing attacks, or compromised accounts, alleged to have been committee by the State. Reporters without Borders, for example, will highlight such attacks where they exist.

75. *Indicator 2.3.6.* stems from the jurisprudence of the ECtHR and Declaration of the Committee of Ministers on the protection of journalism and safety of journalists and other media actors. The latter states that "eradicating impunity is a crucial obligation upon States, as a matter of justice for the victims, as a deterrent with respect to future human rights violations and in order to uphold the rule of law and public trust in the justice system.7 All attacks on journalists and other media actors should be vigorously investigated in a timely fashion and the perpetrators prosecuted. The effective investigation of such attacks requires that any possible link to journalistic activities be duly taken into account in a transparent manner.

76. *Indicator 2.3.7*. concerns the protection of network neutrality as an important condition for the exercise of the right to access to information or the right to freedom of expression. Internet service providers (ISPs) have the ability to manage information and data flows transiting through their networks. The right to access Internet content is linked to the right to receive and impart information on the Internet as referred to in Article 10 of the ECHR. The Council of Europe's Committee of Ministers has affirmed that every Internet user should have the greatest possible access to Internet-based content, applications and services of his/her choice, whether or not they are offered free of charge, using suitable devices of his/her choice. This is a general principle commonly referred to as 'network neutrality' which should apply irrespective of the infrastructure or the network used for Internet connectivity. Verification of this indicator could be found if a positive net neutrality law or policy exists. Negative verification will be found in reports such as those from NGOs, for example Freedom House or from Reporters without Borders, which also cover the use of traffic management to block content.

2.4. Legality, legitimacy and proportionality of restrictions

77. *Indicator 2.4.1*. asks States to verify that any restrictions are in compliance with the requirements of Article 10 paragraph 2 of the ECHR. It should be read together in sections 2.1. and 2.2. Any interference must be prescribed by law. This means that the law must be accessible, clear and sufficiently precise to enable individuals to regulate their behaviour. The law should provide for sufficient safeguards against abusive restrictive measures, including effective control by a court or other independent adjudicatory body. An interference must also pursue a legitimate aim in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary. This list is exhaustive yet its interpretation and scope evolves with the case law of the ECtHR.

78. An interference must also be necessary in a democratic society which means that it should be proven that there is a pressing social need for it, that it pursues a legitimate aim, and that it is the least restrictive means for achieving that aim. In this context, States should asses the balance of laws that restrict Internet content or access against the right to freedom of expression as enshrined in Article 10. In Neij and Sunde Kolmisoppi v. Sweden, the ECtHR has affimed that States must strike a fair balance between the competing rights concerned, as has the Court of Justice of the European Union (CJEU).

79. *Indicator 2.4.2. and 2.4.3* address the specific issue of misuse of law to interfere with the right to freedom of expression and asks States to verify that their laws do not result in a violation of Article 10.

80. Laws, judicial proceedings and other measures taken by State authorities which restrict the right to freedom of expression must meet the standards of Article 10 paragraph 2 of the ECHR. They cannot be justified if their purpose is to prevent free and open public debates, legitimate criticism of public officials or the exposure of official wrongdoing and corruption. An arbitrary application of laws has a chilling effect on the exercise of the right to impart information and ideas and leads to self-censorship.

81. Defamation laws, should be applied with restraint whether offline or online and should have adequate safeguards for freedom of expression. The Court has consistently applied a high threshold of tolerance for criticism where politicians, members of the government or heads of state are concerned. Moreover, the Court has held that criminal sanctions applied in defamation proceedings have a disproportionate chilling effect on the exercise of journalistic freedom of expression. Imprisonment is recognised as a particularly severe sanction and therefore can be applied only exceptionally when the fundamental rights of other have been seriously impaired such as in cases of incitement to violence or hatred. In practice, the Court has not upheld an actual sentence of imprisonment for defamation. The Parliamentary Assembly and the Commissioner for Human Rights have gone one step further by calling for decriminalisation of defamation. Laws and practices providing for disproportionate awards of damages or legal costs in defamation cases may also impinge on freedom of expression.

82. The Venice Commission and the Parliamentary Assembly have taken the view that pluralism, tolerance and broadmindedness in a democratic society require protection of the right to hold specific beliefs or opinions rather than protection of belief systems from criticism. The right to freedom of expression implies scrutiny, open debate and criticism, even harshly and unreasonably, of belief systems, opinions and institutions as long as this does not amount to advocating hatred against an individual or groups of people.

83. Laws which criminalise the spreading, incitement, promotion or justification of hatred and intolerance (including religious intolerance) must be clear as to their application and the restrictions they impose must be proportionate to the legitimate aim pursued in line with the jurisprudence of the Court.

84. Laws on public safety and national security, including those on anti-hooliganism, anti-extremism and anti-terrorism, may restrict the right to receive and impart information both offline and online. It is therefore necessary that such laws are accessible, unambiguous, drawn narrowly and with precision so as to enable individuals to understand what sanctions they face. These laws should also have adequate safeguards against abuse, including prompt, full and effective scrutiny of the validity of restrictions by an independent court or authority. If criminal law sanctions are imposed they must be strictly necessary and proportionate to the legitimate aim pursued as interpreted by the Court.

4. The right to freedom of assembly and association

85. *Indicator 3.1*. seeks to affirm that the State guarantees the application of Article 11 of the ECHR in the context of the Internet and specifically to Internet platforms, social media and applications. The exercise of this right is not conditional upon any formal recognition of social groups and assemblies by public authorities. It includes the right to peacefully assemble and associate with others using the Internet, such as forming, joining, mobilising and participating in societal groups and assemblies, including in trade unions, using Internet-based tools. The indicator will be verified by the existence of constitutional provisions, laws, policies that are in line with international standards on freedom of assembly and association, and where it is understood that those provisions, laws and policies guarantee that right in the context of the Internet and online communication. Negative verification may be found by consulting reports non-governmental organisations, such as the country reports published by Venice Commission or those by non-governmental organisations Article 19.

86. *Indicator 3.2*. seeks to affirm that associations which might be established in offline environments can use the Internet for purposes of their activities. The Joint Guidelines on Freedom of Association of the Venice Commission and OSCE/ODIHR state: "(i)n particular, new

technologies have enhanced the ability of persons and groups of persons to form, join and participate in all forms of associations, including non-governmental organizations and political parties. (…) Many of the traditional activities undertaken by political parties, non-governmental organizations and other associations can be exercised online. These activities can include registering, gathering signatures, fundraising and making donations."

87. Also, individuals should be able to participate in local, national and global public policy debates online, including the free discussion of legislative initiatives and public scrutiny of State decision-making. The indicator is based on Committee of Ministers' recommendations on the public service value of the Internet, which encourage the use of online forums, weblogs, political chats, instant messaging and other forms of citizen-to-citizen communication online, to engage in democratic deliberations, e-activism and e-campaigning, put forward their concerns, ideas and initiatives, promote dialogue and deliberation with representatives and government, and to scrutinise officials and politicians in matters of public interest. An example of the online application of Article 11 in this context would be the signing of a petition or the participation in a campaign of civic action.

88. A form of verification of this indicator would be to assess the development and implementation of strategies for e-democracy, e-participation and e-government using the Internet and internet-based platforms such as social media or other online services, in democratic processes and debates, as recommended by the Committee of Ministers. Such e-democracy strategies could be applied both in relationships between public authorities and civil society, as well as in the provision of public services.

89. *Indicators 3.3. and 3.4.* seek to verify that any restriction on Internet platforms, social media or other online services that facilitate assembly and association complies with Article 11 of the ECHR. In this context, States should take note that the principles established by the ECtHR regarding the protection of political speech under Article 10, also apply to Article 11. In Wingrove v. the United Kingdom, the ECtHR asserted that there is little scope under for State restrictions on either political speech or debates of questions of public interest. Verification would be established if there are no laws or policies, nor any other measures, imposing restrictions on access to or use of Internet platforms, social media or other online services for the purpose of associating with others or creating communities of interest. Verification could be that a restriction has been prescribed by law, with provision for judicial or administrative oversight, including the right to be heard.

5. The right to a private life

4.1. Personal data protection

90. *Indicator 4.1.1* asserts the right to a private and family life, home, and correspondence. This right must be guaranteed by States in compliance with Article 8 of the ECHR. It is interpreted by the case-law of the ECtHR and complemented and reinforced by the Council of Europe Convention 108. The right to private correspondence includes mail and telephone communications, as established in the case of Klass v Germany. In Copland v United Kingdom, the ECtHR has interpreted Article 8 to encompass email correspondence, including in the workplace, as well as information derived from personal internet usage . It has further stated that private life relates to a person's right to their image , for example by means of photographs and video-clips. It also concerns a person's identity and personal development, the right to establish and develop relationships with other human beings. Activities of a professional or business nature are also covered.

91. *Indicator 4.1.2*. addresses the protection of personal data, as defined in Convention 108 for the Protection of Individuals with Regard to the Processing of Personal Data . The indicator seeks to verify that States have assured the protection of personal data within the wider scope of their obligation to safeguard the right to private and family life. The protection of personal data therefore plays a fundamental role in the exercise of the right to respect for private and family life enshrined in Article 8, whereby national legislation must provide appropriate safeguards to prevent any use of personal data which does not comply with the guarantees

provided for in this article and to ensure the effective protection of recorded personal data against misuse and abuse.

92. *Indicator 4.1.3.* seeks to verify that the principles and rules of Convention 108 are respected by public authorities and private companies. Personal data must be obtained and processed fairly and lawfully, and stored for specified and legitimate purposes. Data should be adequate, relevant and not excessive in relation to the purposes for which they are stored, accurate and, where necessary, kept up to date, preserved in a way which permits identification of the person whose personal data are processed and for no longer than is required for the purpose for which those data are stored.

93. Emphasis is placed on two specific principles of the processing of personal data: the lawfulness of the processing, and the user's consent. Convention 108 establishes that users should be able to exercise control over their personal data, notably that they have the right to obtain rectification or erasure of data that has been processed contrary to the law and the right to a remedy if a request for confirmation, rectification or erasure is not complied with.

94. Convention 108 encompasses all forms of data processing that may take place in the context of the Internet - both network and content - such as collection, storage, alteration, erasure and retrieval or dissemination or personal data. In practice, this could include the automatic processing of personal data regarding the use of browsers, e-mail, instant messages, voice-over Internet protocols, social networks and search engines as well as cloud data storage services.

95. Informed consent is underlined in the 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. In particular, social networks should secure the informed consent of their users before their personal data is disseminated or shared, or used in ways other than those necessary for the specified purposes for which they were originally collected. Social network users should be able to "opt in" to permit a wider access to their personal data by third parties (e.g. when third party applications are operated on the social network). Equally, users should also be able to withdraw their consent. This indicator may be verified by the existence of any law that addresses the processing of personal data and incorporates the principles and safeguards enshrined in Convention 108. The free, specific, informed and explicit (unambiguous) consent to the processing of personal data on the Internet is asserted in the Propositions of Modernisation to Convention 108 adopted 18.12. 2012.

96. *Indicators 4.1.4. - 4.1.7.* seek to verify that individuals are capable of exercising their rights in the context of personal data processing. Internet users should be able to exercise control over their personal data as developed in Convention 108, notably the right to obtain rectification or erasure of data that has been processed contrary to the law and the right to a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to above is not complied with. In the context of profiling , the user should also be able to object to the use of his/her personal data for the purpose of profiling and to object to a decision taken on the sole basis of profiling, which has legal effects concerning him/her or significantly affects him/her, unless this is provided by law which lays down measures to safeguard the users' legitimate interests, particularly by allowing him/her to put forward his point of view and unless the decision was taken in the course of the performance of a contract and provided that the measures for safeguarding the legitimate interests of the Internet user are in place. Verification may be carried out by for example examining the compatibility of the terms and conditions of service and platform providers with the law and with the requirements of Article 8.

97. *Indicator 4.1.6.* in particular concerns the issue of anonymity. This is based on the case law of the ECtHR, the Budapest Convention and other instruments of the Committee of Ministers. The ECtHR considered the issue of confidentiality of Internet communications in a case involving the failure of a Council of Europe member state to compel an Internet service provider to disclose the identity of a person who placed an indecent advertisement concerning a minor on an Internet dating website. The ECtHR held that although freedom of expression and confidentiality of communications are primary considerations and users of

telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield, on occasion, to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others. The state has a positive obligation to provide a framework which reconciles those competing interests.

98. The Budapest Convention does not criminalise the use of computer technology for purposes of anonymous communication. According to its explanatory report, "the modification of traffic data for the purpose of facilitating anonymous communications (e.g. activities of anonymous remailer systems) or the modification of data for the purposes of secure communications (e.g. encryption) should in principle be considered a legitimate protection of privacy, and, therefore, be considered as being undertaken with right. However, Parties [to the Budapest Convention] may wish to criminalise certain abuses related to anonymous communications, such as where the packet header information is altered in order to conceal the identity of the perpetrator in committing a crime."

99. The Council of Europe's Committee of Ministers affirmed the principle of anonymity in its Declaration on Freedom of Communication on the Internet. Accordingly, in order to ensure protection against online surveillance and to enhance freedom of expression, Council of Europe member States should respect the will of Internet users not to disclose their identity. However, respect for anonymity does not prevent member States from taking measures in order to trace those responsible for criminal acts, in accordance with national law, the ECHR and other international agreements in the fields of justice and the police.

100. This indicator may be negatively verified by the existence of any law or policy prohibiting Internet users to use encryption software to protect their communications, or by any law or policy restricting the use of encryption or other security software or enabling the government agencies to have access to encryption keys and algorithms. Positive verification entails the absence of such laws or policies.

4.2. Freedom from surveillance

101. *Indicator 4.2.1.* draws on the jurisprudence of the ECtHR. It seeks to verify that all surveillance measures comply with Article 8 of the ECHR and are subject to independent and impartial oversight. Surveillance measures can be both general (mass surveillance) or targeted. The ECtHR has interpreted Article 8 such that the concept of correspondence covers mail and telecommunications as well as e-mails . The interpretation of this concept of correspondence is evolving to keep pace with technology development. Guaranteeing the confidentiality of communications entails protecting them from all forms of surveillance, including interception. In the context of the Internet, surveillance relates to the listening to, recording, monitoring or storing of private communications. It may involve securing the content of data – this could be done by obtaining covert access to systems, or by means of electronic eavesdropping or tapping devices. Surveillance in the Internet context may additionally entail the gathering, storage and analysis of communications traffic data or metadata. This is data which does not reveal the content of the communication, but does reveal the sender, transmission details, and subject of it.

102. The ECtHR interpreted Article 8 of the ECHR in the context of surveillance cases has pronounced itself on the importance of supervision of surveillance measures by authorities other than those who carry out such measures. Although the cases reviewed by the ECtHR do not concern Internet technologies the principles established therein are valid in the context of the Internet. This is based on the general principle established by the ECtRH that "[it] must be satisfied that, whatever system of surveillance is adopted, there exist adequate and effective guarantees against abuse". The review of surveillance may intervene at three stages: when the surveillance is first ordered, while it is being carried out, or after it has been terminated. The ECtHR has derived from the general principle of the rule of law that, in the context of surveillance, an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in

the last resort, judicial control offering the best guarantees of independence, impartiality and a proper procedure.

103 *Indicator 4.2.2*. seeks to verify that any form of State interception or surveillance of private correspondence or activities on the Internet must have a basis in law. However, a law that institutes a system of surveillance, under which all persons in the country concerned can potentially have their mail and telecommunications monitored, directly affects all users or potential users of the postal and telecommunication services in that country. Hence, the very existence of legislation permitting surveillance of telecommunications may be considered as an interference with the right to private life. The EctHR has accepted that an individual may, under certain conditions, claim to be the victim of a violation occasioned by the mere existence of secret measures or of legislation permitting them, without having to allege that such measures were in fact applied to him or her.

104. These principles established by the ECtHR make particular reference to the requirements that should be met by any law that provides for covert measures of surveillance of correspondence and communications by public authorities. The law should have detailed rules on minimum safeguards for the exercise of discretion by public authorities. These minimum safeguards include rules on (i) the nature of the offences which may give rise to an interception order; (ii) the definition of the categories of people liable to have their communications monitored; (iii) the limit on the duration of such monitoring; (iv) the procedure to be followed for examining, using and storing the data obtained; and (v) the precautions to be taken when communicating the data to other parties; (vi) the circumstances in which data obtained may or must be erased or the records destroyed.

105. Verification of this indicator is therefore done on the basis not only of the existence of a law, but also of the quality of the law, which must incorporate safeguards against abuse . It should enshrine the principle of foreseeability, namely that the law must be accessible to the person concerned who must be able to foresee the consequences of its application to him/her. The law must also be formulated with sufficient clarity and precision to give citizens an adequate indication of the conditions and circumstances in which the authorities are empowered to resort to covert and potentially harmful interference with the right to respect for private life and correspondence. Verification may be obtained from reports of international organisations, bodies such as the Council of Europe Commissioner for Human Rights, the Venice Commission, and the United Nations special rapporteur on freedom of expression as well as NGOs such as Reporters without Borders, Freedom House, Article 19, and Index on Censorship.

106. *Indicator 4.2.2*. seeks to establish that any law or policy implementing surveillance measures will pursue a legitimate public policy aim in line with those Article 8 paragraph 2. This aim should be precisely defined and narrow in scope. This indicator also refers to paragraph 2 of Article 8 which requires that any surveillance law or policy, or order, is necessary in a democratic society . This means that it should be proven that there is a pressing social need for it, and that it is the least restrictive means for achieving that aim. The necessity of such a law requires that the aim is balanced against competing rights and freedoms. The indicator seeks to establish that such a balancing process has been conducted.

107. This indicator draws from the ECtHR jurisprudence, which has underlined that such measures can only be considered "necessary in a democratic society" if the particular system of secret surveillance adopted contains adequate guarantees against abuse'. The ECtHR held that although measures which interfere with privacy may be designed to protect democracy, they carry with them an inherent possibility for abuse of power that could have harmful consequences for democracy as a whole. Negative verification may be obtained from reports covering State surveillance that appears not to pursue a legitimate aim. These reports may come from international organisations as well as NGOs, for instance Article 19, Freedom House, Index on Censorship and Reporters Without Borders.

108. *Indicator 4.2.3.* is based on the jurisprudence of the ECtHR which requires that whenever a State puts in place a system of surveillance there are effective guarantees against abuse.

The ECtHR has acknowledged that the States enjoy a certain margin of appreciation in assessing the existence and extent of such necessity, but this margin is subject to European supervision. The ECtHR has to determine whether the procedures for supervising the ordering and implementation of the restrictive measures are such as to keep the interference to what is necessary in a democratic society.

109. This indicator focuses on the prior authorisation of surveillance measures. The ECtHR has expressed a preference for judicial authorisation of surveillance measures. Despite the fact that the ECtHR has not made prior judicial authorisation a requirement applicable to all cases, its jurisprudence clearly requires that the body authorising surveillance measures should be independent of the service carrying out surveillance measures and the executive.

110. Verification of this indicator may be found in the existence of mechanisms for supervision and review by competent authorities, such as Parliamentary committees or other public bodies responsible for such oversight. These public bodies should be independent of the executive and of any authorities charged with conducting surveillance.

111. *Indicators 4.2.5. to 4.2.7.* seek to verify that there is adequate oversight of surveillance measures during or after the phase of their implementation. These are derived from the criteria that the ECtHR has used to asses whether or not oversight arrangements provide sufficient safeguards to prevent abuse. The ECtHR has consistently held that the review of surveillance measures should be done by an independent body. There must be a legal basis which explains how such supervision is carried out. The ECtHR had identified competences of oversight bodies that would be relevant to an assessment of effective safeguards against abuse. Among the criteria that the ECtHR has examined is whether oversight bodies have access to all relevant information, including classified information and whether they have the power to quash surveillance orders and require that the material obtained through surveillance measures is destroyed.

112. *Indicators 4.2.8 to 4.2.10.* are drawn from the recommendations of the Council of Europe Human Rights Commissioner regarding the democratic oversight of national security services. The Commissioner stresses that the mandate of such bodies should include scrutiny of human rights compliance of security services co-operation with foreign bodies, including co-operation through the exchange of information, joint operations and the provision of equipment and training. External oversight of such co-operation with foreign bodies should include, "a. ministerial directives and internal regulations relating to international intelligence co-operation; b. human rights risk assessment and risk-management processes relating to relationships with specific foreign security services and to specific instances of operational co-operation; c. outgoing personal data and any caveats (conditions) attached thereto; d. security service requests made to foreign partners: (i) for information on specific persons; and (ii) to place specific persons under surveillance; e. intelligence co-operation agreements; f. joint surveillance operations and programmes undertaken with foreign partners."

113. Verification may be found in the existence of mechanisms for supervision and review by competent authorities, such as Parliamentary committees or other public bodies responsible for such oversight.

5.Remedies

114. *Indicator 5.1*. seeks to verify that Internet users are able to exercise their right to fair trial, which is enshrined in Article 6 of the ECHR. This refers to the determination of civil rights and obligations or criminal charges with regard to activities of Internet users. In particular, this concerns key principles pronounced by the ECtHR, namely the right to a fair and public hearing within a reasonable time by an independent and impartial court; the right to institute proceedings before courts, to a final determination of the dispute, to a reasoned judgment and to the execution of the judgment; the right to adversarial proceedings and equality of arms and others. The ECtHR, although not in Internet-related cases, has established general principles with regard to the quality of administration of justice (independence, impartiality, competence of the tribunal), the protection of right of the parties (fair hearing, equality of

arms and public hearing) as well as with regard to the efficiency of justice administration (reasonable time).

115. There should be a national authority tasked with arbitrating on allegations of such violations of the rights guaranteed. The authority may not necessarily be a judicial authority if it presents guarantees of independence and impartiality. However, its powers and the procedural guarantees afforded should permit a determination whether a particular remedy is effective. The procedure followed by the competent national authority should permit effective investigation of a violation. It should allow the competent authority to decide on the merits of the complaint of a violation of ECHR rights, to sanction any violation and to guarantee the victim that the decision taken will be executed. The legal procedure should be complemented by a specific legal avenue available whereby an individual can complain about the unreasonable length of proceedings in the determination of his/her rights.

116. *Indicators 5.2. and 5.3*. seek to verify that the right to an effective remedy as enshrined in Article 13 of the ECHR is respected. Everyone whose rights and freedoms are restricted or violated on the Internet has the right to an effective remedy. These indicators are based on the jurisprudence of the ECtHR. States, as part of their positive obligations to protect individuals against violations of human rights by private companies, should take appropriate steps to ensure that when such violations occur those affected have access to judicial and non-judicial mechanisms. This indicator concerns ECHR Article 13, which guarantees the availability, at the national level, of a remedy to enforce the substance of ECHR rights and freedoms in whatever form they might happen to be secured in the domestic legal order. Article 13 requires the provision of a domestic remedy to deal with the substance of a complaint under the ECHR and to grant appropriate relief. States have a positive obligation to carry out an investigation of allegations of human rights infringement that is diligent, thorough and effective. The procedures followed must enable the competent body to decide on the merits of the complaint of violation of the Convention and to sanction any violation found but also to guarantee the execution of decisions taken.

117. The remedy must be effective in practice and in law and not conditional upon the certainty of a favourable outcome for the complainant. Although no single remedy may itself entirely satisfy the requirements of Article 13, the aggregate of remedies provided in law may do so. Effective remedies should be available, known, accessible, affordable and capable of providing appropriate redress. Public authorities and/or other national human rights institutions may be in a position to apply an effective remedy. In the context of the Internet, broadband service providers may also be in a position, but they do not enjoy sufficient independence to be compatible with Article 13 ECHR.

118. *Indicator 5.4.* seeks to verify the implementation of the United Nations Guiding Principles on Business and Human Right, which specify that companies should establish complaint mechanisms which are accessible, predictable (providing clear and known procedure with indication of time frames for each stage of the process, clarity on the types of process and outcomes available and the means for monitoring their implementation) equitable (access to sources of information, advice and expertise), transparent and capable to offer remedies which are in full compliance with international human rights standards directly to individuals.

119. Verification may be sought in the terms of use and services of Internet platforms with a view to establishing whether Internet users are offered clear and transparent information regarding the means of redress available to them. Internet users should be provided with practical and accessible tools to contact Internet service/online providers to report their concerns. They should be able to request information and seek remediation. Some examples of remedies which may be available to Internet users are helplines or hotlines run by Internet service providers or consumer protection associations to which Internet users can turn in the case of violation of their rights or the human rights of others. Guidance should be provided by public authorities and/or other national human rights institutions (ombudspersons), data protection authorities, regulators for electronic communications, citizens' advice offices, human rights or digital rights associations or consumer organisations.

120. Other sources of verification include transparency reports issued by the Internet Service Providers or by the Internet platforms. Google provides Transparency reports detailing removal requests from its search engine, blogging platform and YouTube. The removal requests come from State authorities and law enforcement, and from copyright holders. With regard to copyright, Google provides names of those making the request and the requested URL. With regard to government removal requests, Google provides generic information, without disclosing any names. Twitter publishes transparency reports regarding law enforcement and government requests for removal of content, and also reports on requests for removal of content under US copyright law. Twitter provides aggregated figures only, with no details of the individual requests. Vodafone provides a country-by-country-disclosure report on the assistance that it provides to law enforcement, with additional details on certain countries in an Annexe. It provides information on how it handles requests for content removal, following the UN guidelines for business and human rights, but it does not disclose the actual requests. Other sources of verification may be reports from international human rights organisations that have analysed Internet blocking orders.

121. Transparency reports provided by intermediaries provide some means of verification, although the actual data published may be limited to total numbers of requests made and the number of requests complied with. Google provides Transparency reports detailing the number of government requests for information about its users. Twitter publishes transparency reports on law enforcement and government requests for data related to its users. Facebook discloses transparency reports on law enforcement requests for personal data of its users. Vodafone provides a transparency report on which governments require it to disclose communications traffic data and the legal basis for doing so.

APPENDIX V

Internet Governance Strategy 2016-2019[1]

Democracy, human rights and the rule of law in the digital world

Final draft

Introduction

1. The Internet is increasingly significant in the everyday activities of European citizens. It should be a safe, secure, open and enabling environment for everyone without discrimination[2]. Everyone must be able to exercise their human rights and fundamental freedoms online as well as offline, including the right to private life and the protection of personal data, subject, in certain cases, to narrowly circumscribed restrictions. They should be protected from crime and insecurity online and from unlawful surveillance of their activities. They should be free to communicate without censorship or other interference, and they should feel confident about sharing their personal data, creating and participating on-line. As a tool and public space for democracy, Internet governance should enable dialogue and interaction between all segments of the population to promote respect, equality, tolerance, and living together thereby fostering engagement and participation in a democratic society. Above all, the Internet should remain universal, innovative, and continue to serve the interests of users. It is a global resource, the integrity of which should be protected and managed in the public interest. The Council of Europe should promote the full inclusion of all stakeholders, in their respective roles, in Internet governance.

A continuum of core values

2. The strategy on Internet governance 2012-2015 brought together relevant Council of Europe standards and monitoring, co-operation and capacity-building activities. The strategy linked legally-binding treaties, such as the 'Budapest'[3], 'Istanbul'[4] and 'Lanzarote'[5] Conventions, the transversal strategies on gender equality and children's rights, the dynamic platform for youth participation, and led to the Guide to human rights for Internet users. It enabled member States to debate the cultural challenges of the Internet. It also facilitated better in-house co-ordination in the Council of Europe.

3. The Council of Europe is recognised for its work on protecting the Internet's universality, integrity and openness. It has reasserted the need to protect and empower citizens without chilling their freedom to use the Internet for everyday activities. The public service value of the Internet, in particular the legitimate expectations of Internet users, were recognised. The Organisation was also connected with a large number of public and private actors at European and global levels, and able to deliver important messages, such as 'doing no harm' to the Internet and 'no hate' online.

[1] The Russian Federation does not approve of the draft.

[2] They must not be discriminated against 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 (Para 4 of the Appendix to CM Recommendation on the Guide to Human Rights for Internet Users).

[3] Council of Europe Convention on Cybercrime (ETS No. 185).
[4] Council of Europe Convention on preventing and combating violence against women and domestic violence (CETS No.: 210).
[5] Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201).

Aims and objectives

4. The strategy is a multi-disciplinary tool which covers issues concerning content, services and connected devices running over the Internet, including relevant aspects of its infrastructure and functioning which can affect human rights and fundamental freedoms. The strategy identifies many challenges to the internet and provides governments and other stakeholders, including civil society, the private sector, technical and academic communities, with means to address them.

5. Its overall aim is to ensure that public policy for the Internet is people-centred, meaning that it should respect the core values of democracy, human rights and the rule of law. Its strategic objectives are to build democracy online, to protect Internet users, and to ensure respect and protection for human rights online. To this end, the strategy proposes a series of specific activities.

Strategic objectives

Building democracy online

6. The Internet is of critical value for democracy. Its capacity to allow people to impart and exchange their ideas, knowledge and opinions as well as to share and store vast amounts of information is unprecedented and offers the potential to promote understanding and tolerance between people of diverse cultures, backgrounds and of different beliefs. The Internet provides opportunities for the inclusion and participation of all people without discrimination and helps to connect those who may feel vulnerable or marginalised thereby making it easier for them to access public services. Connecting their voices to the Internet, including those living in geographically remote or underdeveloped areas and persons with disabilities, is important for pluralism and diversity in dialogue, and for bridging the gaps in dialogue between states and citizens.

7. Beyond the deployment of e-democracy and e-voting, e-government and e-justice initiatives, the Internet's public service value should be developed further. This includes enabling online participation in public life, also at local level, which respects the privacy (and freedom from mass surveillance) of citizens while ensuring that any personal information processed is not mismanaged or misused. Pre-requisites for building democracy online include access to both sustainable digital culture and authentic digital content and access to public documents and data. Also important is the introduction of new approaches to public administration and service delivery to enhance e-governance at the local level, and of innovative methods of engaging and participating in the democratic process. It is important to introduce digital citizenship education into formal education systems as part of the official curriculum. It further means encouraging citizens to engage with digital culture and benefit from its potential for inclusion and innovation as well as to develop a healthy and balanced relationship with the Internet, one which is based on the freedom to connect but also to disconnect (i.e. the so-called 'digital detox').

8. In this context, the Council of Europe will:

   a. Further develop its network of (digital) democracy innovators in the framework of the World Forum for Democracy. Future Forum topics for consideration include the future of the Internet and its governance, the use of digital tools for greater efficiency and accountability, citizen participation and transparency in democracy, a possible 'Magna Carta' for the Internet, and 'net-citizenship'.

   b. Explore ways and propose concrete measures to prevent and address hate speech online, including speech which leads to violence. This comprises awareness campaigns to prevent and address manifestations of hate towards any member or group in society and the continuation of the No Hate Speech campaign.

c. Launch a consultation and survey on European formal and non-formal education, critical knowledge, skills and attitudes in the digital world, with a view to preparing a whitepaper on media and information literacy. Guidelines for digital citizenship education in European schools, the creation of a network of European 'digizen' schools and digital badges for democratic skills based on the framework of competences for democratic culture will also be developed.

d. Having regard to international consensus on the importance of the transition from the information society to the knowledge society, actively promote the principle of multilingualism in the fostering of linguistic and cultural diversity.

e. Promote the role of youth work in fostering online participation, media and digital literacy of youth, including the marginalised and hard to reach

f. Continue to strengthen European dialogue and good practice exchange on the creation, access and management of digital culture to promote citizen engagement, openness, inclusion and tolerance in democratic societies. This includes the organisation of multi-stakeholder platform exchanges, preparation of policy guidelines for member States, cultural institutions and practitioners and the development of an interactive website on the Internet of Citizens.

Ensuring online safety and security for all

9. The online safety and security of Internet users is a shared responsibility. This requires action to combat violent extremism and radicalisation, cybercrime, as well as the exploitation, harassment and bullying of people using the Internet. This also includes the protection against sexual abuse and exploitation of children online, action to fight organ and human trafficking, and the sale of counterfeit medicines and drugs. A continuous effort to address these threats remains vital provided that measures taken are subject to conditions and safeguards for the adequate protection of human rights and fundamental freedoms .

10. In this context, the Council of Europe will:

a. Continue to promote the Budapest Convention on Cybercrime and 'Convention 108' on data protection[6] as Council of Europe global standards' and promote accession by a maximum number of countries worldwide. The implementation of the conventions requires capacity building and the fostering international co-operation, This also includes the setting up of common Internet governance policies and principles including in the field of network and information security.

b. Steward debate and propose concrete measures to address the concerns about mass surveillance and the bulk interception of data, for example the creation of built-in flaws and backdoors in security information and communication systems, as well as the challenges for the protection of personal data and human rights generally, while ensuring security and safety.

c. Develop a strategy to counter violent extremism and radicalisation on the Internet which covers all level of government, carried out in synergy with the Council of Europe Action Plan for 2015-2017, and the Convention on the Prevention of Terrorism including its Additional Protocol on "foreign terrorist fighters".

d. Monitor action taken to protect everyone, in particular women and children, from online abuse, such as cyber-stalking, sexism and threats of sexual violence.

[6] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108).

Respecting and protecting the human rights of everyone in the digital world

11. Individuals rely on the Internet for their everyday activities and it is welcomed that more and more people have access to online services. For many, including children and young people, it is their primary means of information and expression. The Internet is therefore an invaluable space for the exercise of fundamental rights such as freedom of expression and information. Moreover, better awareness is needed of legitimate expectations and restrictions when using Internet services, and how to seek redress and remedies when human rights have been violated. The important role played by media and new media actors, as enablers of access to pluralistic and diverse information should be underlined whilst remaining mindful of the possibilities to discriminate Internet traffic and interfere with content generally.

12. There are increasing risks to the human rights of Internet users as it becomes easier to connect or to be connected to the Internet and information and communication technologies (ICTs) using every day (household) devices and objects (e.g. cars), often referred to as the 'Internet of Things'. Digital tracking and surveillance, the collection of personal data, including sensitive data related to health, for the purposes of profiling pose a threat to privacy and the general enjoyment of human rights including freedom of expression and access to information. Anonymity and encryption tools can help Internet users protect themselves against these threats although respecting their will not to disclose their identities should not prevent member States from taking measures and co-operating in order to trace those responsible for criminal acts.

13. In this context, the Council of Europe will:

    a. Promote the setting-up of a network of national institutions to guide Internet users who seek redress and remedies when their human rights have been restricted or violated based on the Council of Europe Guide to human rights of Internet users. This includes cooperation assistance in raising awareness and developing tools to build capacity.

    b. Conduct triennial reporting on the state of data protection and privacy on the Internet in Europe, having regard to the (modernised) 'Convention 108' on data protection.

    c. Develop policy on the role of intermediaries and their importance for freedom of expression and media freedom in the light of the case-law of the European Court of Human Rights and taking into account best practice in blocking, filtering and takedown of Internet content.

    d. Periodically report on the state of media and Internet freedom in line with Council of Europe standards, in particular by means of the Council of Europe platform for the safety and protection of journalism and the reports of the Secretary General on freedom of expression in Europe.

    e. Establish a platform between governments and major Internet companies and representative associations on their respect for human rights online, including on measures (such as model contractual arrangements for the terms of service of Internet platforms, and principles of accountability and transparency to the multi-stakeholder community regarding the collection, storage and analysis of personal data) to protect, respect and remedy challenges and violations to them.

    f. Assess and review, in cooperation with governments, the European Commission, and other Internet governance stakeholders, the governance of mobile health ('mHealth') and electronic health ('eHealth'), in order to preserve and improve the access of patients to all available (quality) health and healthcare products, as well as information and related services. This includes consideration of ways to prevent

the illegal sale of drugs and counterfeit medicines as well as illicit trafficking in drugs online.

Partnerships and synergies

14. The Council of Europe recognises and is firmly committed to cooperating with leading actors in the field of Internet governance, including relevant international organisations, the private sector, and civil society. It is also supportive of the work of other Internet governance stakeholders who help to shape public policy for the Internet.

15. The effective protection and promotion of democracy, human rights and the rule of law in the digital world is a shared task and a common goal between many stakeholders. This necessitates partnerships and synergies with and between states, international organisations, civil society, the private sector, technical and academic communities. The Council of Europe will therefore review, strengthen and develop synergies and partnerships with key stakeholders, including the following:

    a. European Union;
    b. Organisation for Security and Cooperation in Europe (OSCE);
    c. Organisation for Economic Cooperation and Development (OECD);
    d. United Nations and its agencies, including those involved in the follow-up and implementation of the World Summit on the Information Society (WSIS): UN Educational, Scientific and Cultural Organisation (UNESCO), Office of the High Commissioner for Human Rights UN Office on Drugs and Crime (UNODC), and the International Telecommunication Union (ITU);
    e. Organisations, networks and initiatives on cybercrime and cybersecurity such as Europol, Interpol, the Virtual Global Task Force, Commonwealth and others;
    f. European Broadcasting Union;
    g. World Bank;
    h. Internet governance networks and bodies, including the European Dialogue on Internet Governance (EuroDIG), the Internet Governance Forum (IGF), the Internet Corporation for Assigned Names and Numbers (ICANN), national Internet governance initiatives, 'Freedom Online Coalition', 'London Process', 'NETmundial Initiative', and the Internet Society (ISOC);
    i. Private sector, and representative associations including European Internet Service Providers Association (EuroISPA).
    j. European Youth Forum, and related youth networks.
    k. Cultural networks and representative professional associations such as CultureActionEurope.
    l. Research communities.

Working methods and budgetary implications

16. In line with the European Convention on Human Rights and the jurisprudence of the European Court of Human Rights, the Council of Europe's legally-binding treaties and mechanisms, and, where appropriate, in conjunction with the Parliamentary Assembly, Congress of Local and Regional Authorities, Conference of INGOs, and Commissioner for Human Rights, the Council of Europe will implement the strategy through its steering and convention committees, transversal strategies on gender equality, children's rights, monitoring bodies, commissions, networks including the national committees of the 'No Hate' Speech campaign, cooperation and capacity building programmes of activities, and by the action of its Secretariat. This will include ongoing assessment of the legal instruments and other work of relevance to Internet governance.

17. The strategy will span two biennium budgetary cycles of the Council of Europe (2016-17 and 2018-19). The implementation of its key actions and activities are in line with the priorities of the Secretary General for 2016-17 (see document CM(2015)81) as

reflected in the programme and budget of the Council of Europe for 2016-2017. Extra budgetary resources and joint programme funding may also be used.

Planning, implementation and evaluation of the strategy

18. The strategy will be carried out by the relevant steering and convention committees of the Council of Europe as well as through its networks and platforms of inter alia young people, NGOs, public authorities, and legal professionals. Oversight of the implementation of the strategy will be the responsibility of the Steering Committee on Media and Information Society (CDMSI) in close co-operation with the Thematic Co-ordinator for Information Policy (TC-INF) of the Committee of Ministers.

19. The Secretary General will ensure the strategic planning, implementation and evaluation of the strategy.

20. Similarly, the Secretary General will ensure that work relating to Internet governance is prepared in consultation with relevant stakeholders. These processes will be gender balanced and as inclusive as possible building on good practices.

21. Transversal working methods will be developed, where necessary, to facilitate the delivery of the strategic objectives. Best practice and, where appropriate, outstanding action resulting from the Internet governance strategy 2012-2015 will be carried forward.

22. Reviewing progress on the implementation of the strategy will be carried out by the Secretary General, in particular by means of mid-term and final assessment reports to be submitted to the Committee of Ministers for consideration in due course.

Draft Internet Governance Strategy 2016-2019
Glossary of Terms

- **'Digital detox'**: A period of time during which a person refrains from using electronic devices such as smartphones or computers, regarded as an opportunity to reduce stress or focus on social interaction in the physical world[7]

- **European dialogue on Internet governance (EuroDIG)**: EuroDIG is an open multi-stakeholder platform to exchange views about the Internet and how it is governed. Created in 2008 by several organisations, government representatives and experts, it fosters dialogue and collaboration with the Internet community on public policy for the Internet. Culminating in an annual conference that takes place in a different capital city, EuroDIG 'messages' are prepared and presented to the UN-led Internet Governance Forum. EuroDIG is supported by a group of institutional partners, namely the Council of Europe, the European Commission, the Internet Society (ISOC), the European Regional At-Large Organization (EURALO), the European Broadcasting Union (EBU), the Réseaux IP Européens Network Coordination Centre (RIPE NCC) and the Federal Office of Communications of Switzerland (OFCOM).

- **Freedom Online Coalition**: The Freedom Online Coalition is a group of governments who have committed to work together to support Internet freedom and protect fundamental human rights – free expression, association, assembly, and privacy online – worldwide. The Coalition was established in 2011 at the inaugural Freedom Online Conference in The Hague, the Netherlands at the initiative of the Dutch Foreign Ministry. Today the Coalition has 28 members, spanning from Africa to Asia, Europe, the Americas, and the Middle East. All member states signed the FOC founding document (Freedom Online: Joint Action for Free Expression on the Internet) and committed to the principle that the human rights people have offline are the same online. The Coalition members coordinate their diplomatic efforts, share information on violations of human rights online and work together to voice concern over measures that curtail human rights online. The Coalition also collaborates by issuing joint statements, by sharing policy approaches to complex issues, exchanging views on strategy, and planning participation in relevant forums.

- **Internet of citizens**: This refers to the draft Recommendation of the Committee of Ministers of the same name which states that "in addition to investing in the technical and infrastructural aspect of the "internet of things", equal consideration should be given to its cultural dimension and to the "internet of citizens. The term "citizens" is used here in a general sense, meaning people or persons, and not in any legal sense.

- **Internet Corporation for Assigned Names and Numbers (ICANN)**: ICANN is a non-profit responsible for the global coordination of the Internet's unique identifier and its stable operation and safe profit organization[8].

- **Internet governance**: The working definition of Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet.[9]

- **Internet governance forum (IGF)**: In the framework of the UN World Summit on the Information Society (WSIS), in particular paragraph 72 of the Tunis Agenda for the Information Society, the mandate of the Internet Governance Forum is to:

[7] http://www.oxforddictionaries.com/definition/english/digital-detox

[8] https://www.icann.org/en

[9] Report of the Working Group on Internet Governance, Château de Bossey June 2005: http://www.wgig.org/docs/WGIGREPORT.pdfhttp://www.wgig.org/docs/WGIGREPORT.pdf

a. Discuss public policy issues related to key elements of Internet governance in order to foster the sustainability, robustness, security, stability and development of the Internet.
b. Facilitate discourse between bodies dealing with different cross-cutting international public policies regarding the Internet and discuss issues that do not fall within the scope of any existing body.
c. Interface with appropriate intergovernmental organizations and other institutions on matters under their purview.
d. Facilitate the exchange of information and best practices, and in this regard make full use of the expertise of the academic, scientific and technical communities.
e. Advise all stakeholders in proposing ways and means to accelerate the availability and affordability of the Internet in the developing world.
f. Strengthen and enhance the engagement of stakeholders in existing and/or future Internet governance mechanisms, particularly those from developing countries.
g. Identify emerging issues, bring them to the attention of the relevant bodies and the general public, and, where appropriate, make recommendations.
h. Contribute to capacity building for Internet governance in developing countries, drawing fully on local sources of knowledge and expertise.
i. Promote and assess, on an ongoing basis, the embodiment of WSIS principles in Internet governance processes.
j. Discuss, *inter alia*, issues relating to critical Internet resources.
k. Help to find solutions to the issues arising from the use and misuse of the Internet, of particular concern to everyday users.
l. Publish its proceedings.

- **Internet Society (ISOC)**: ISOC is a non-governmental international organization for global cooperation and coordination for the Internet and its internetworking technologies and applications. The Society's individual and organizational members are bound by a common stake in maintaining its viability and global scaling of the Internet. They comprise the companies, government agencies, and foundations that have created the Internet and its technologies as well as innovative new entrepreneurial organizations contributing to maintain that dynamic."[10]

- **'London Process'**: The Global Conference on Cyberspace (also known as the London process) are conferences held each years since 2011 where governments, private sector and civil society gather in order to promote practical cooperation in cyberspace, to enhance cyber capacity building, and to discuss norms for responsible behaviour in cyberspace. The first conference has been hold in November 2011 in London. There, a set of principles "for governing behaviour in cyberspace" have been established after a discussion from 700 participants. The second conference was hold on October 4-5th, 2012 in Budapest. The third event was hold on 17–18 October 2013 in Seoul. The fourth one was hold in World Forum from 16 to 17 April 2015 in The Hague.[11]

- **'Net-citizenship'**: The term 'Netizen' is a portmanteau of the words Internet and citizen as in "citizen of the net". It describes a person actively involved in online communities or the Internet in general. The term commonly also implies an interest and active engagement in improving the Internet, making it an intellectual and a social resource, or its surrounding political structures, especially in regard to open access, net neutrality and free speech. Netizens are also commonly referred to as cybercitizens, which has similar connotations[12].

- **'NETmundial' and the NETmundial Initiative:** The NETmundial meeting held in São Paulo, Brazil, in April 2014, provided a reference for governments, private sector, civil society, technical community and academia from around the world to address Internet governance challenges. Its concluding document (link is external), the NETmundial

[10] http://www.businessdictionary.com/definition/internet-society-ISOC.html
[11] https://en.wikipedia.org/wiki/Global_Conference_on_CyberSpace.
[12] https://en.wikipedia.org/wiki/Netizen

Multistakeholder Statement ("Statement"), recognized that the Internet is a global resource which should be managed in the public interest. It also reaffirmed the importance of human rights to the Internet and provided a set of Internet governance Principles, as well as a Roadmap for the future evolution and improvement of the existing Internet governance framework, ensuring the full involvement of all stakeholders. The NETmundial Initiative ("Initiative") recognizes the NETmundial Internet governance process Principles: democratic, multistakeholder, open, participative, consensus-driven, transparent, accountable, inclusive and equitable, distributed, collaborative, and enabling of meaningful participation. The Initiative seeks to carry forward the cooperative spirit of São Paulo by enabling opportunities for collaboration and cooperation between all stakeholders.[13]

- **Public service value of the Internet**: Derived from the Recommendation CM/Rec(2007)16 of the Committee of Ministers to member states on measures to promote the public service value of the Internet which is "understood as people's significant reliance on the Internet as an essential tool for their everyday activities (communication, information, knowledge, commercial transactions) and the resulting legitimate expectation that Internet services be accessible and affordable, secure, reliable and ongoing".[14]

[13] https://www.netmundial.org/terms-reference
[14] https://wcd.coe.int/ViewDoc.jsp?id=1207291

Draft Internet Governance Strategy 2016-2019 - Appendix of activities

Pillar and theme	Activities	Timeline	Major Administrative Entity
Building democracy online			
E-voting	Update of Council of Europe Recommendation Rec(2004)11 on legal, operational and technical standards for e-voting, and follow-up work on it such as biennial review-meetings, monitoring of compliance in member States, development of complementary guidelines, identification of good practices, technical assistance to member States on the adoption of e-voting system, on awareness-raising and voter education, on work with domestic observers to monitor e-enabled elections		DG2 – Directorate of Democratic Governance, Department on Democratic Institutions and Governance, Division on Elections
Democracy and participation	Presentation and analysis of e-participation platforms in the context of each annual edition of the World forum for democracy Support for the introduction of e-participation platforms at the local and national level, capacity-building and good practice exchange Development and testing of an assessment tool for participatory democracy at the local, including internet-based participation		DG2-Directorate of Democratic Governance, Department on Democratic Initiatives, Division on World Forum for Democracy
No Hate speech	Council of Europe No Hate Speech Campaign will continue its work in 2016-2017 with greater emphasis on education for human rights and digital citizenship and on improving and disseminating reporting and monitoring mechanisms about hate speech. The Campaign has been assigned the main role of prevention of violent extremism and radicalisation leading to terrorism on the Internet in the Council of Europe Action Plan. Counter-narratives will be developed to empower users to respond to or neutralise online hate speech		DG2-Directorate of Democratic Citizenship and Participation, Youth Department, Division on Non-formal Education and Training

	European Commission against Racism and Intolerance (ECRI) to adopt, in early 2016, a General Policy Recommendation on combating hate speech Promote implementation of Protocol to the Budapest Convention on Xenophobia and Racism (ETS 189) as a tool to right hate speech online		DG2-Directorate of Human Dignity and Equality, Anti-Discrimination and Social Cohesion Department, European Commission Against Racism and Intolerance (ECRI) DG1-Directorate of Information Society and Action Against Crime, Information Society Department, Cybercrime Division
Digital citizenship	Conduct a review of formalized literature and informal literature (blogs, wikis and websites), to examine the concept of digital citizenship, current digital education policies and contemporary digital education practices and challenges in schools Organise multi stakeholder consultations/debates on policy issues regarding the place and better use of online resources and contemporary information technologies (Social Networking sites and Web 2.0 or Educational Web 2.0 sites as well as personal devices) in school settings (curricula and schools organisations) and mapping the administrative and legal responsibilities for school leaders, teachers, students and parents Develop policy guidelines to further support national authorities in developing digital citizenship education policies to address learning issues as well as the needs of students, and to provide guidance in policy development to help protect students working in open, collaborative, online environments Promote and share best practices from member states on effective interactive programmes for the acquisition of digital citizenship competence for students through the curriculum, and for teachers through initial and in-service education Based on the experience of member states, establish a set of		DG2-Directorate of Democratic Citizenship and Participation, Education Department, Division on Education Policy

	descriptors for digital citizenship education competence and develop guidance for the integration of such descriptors in current citizenship education curricula Develop, in partnerships with other sectors of the Council of Europe, policy orientations with regard to crosscutting contemporary educational and legal issues that school authorities should face today, such as: cyberbullying (including cyber-misogyny, cyberbullying of teachers), privacy, sexting, digital addiction, students' and teachers' relationships through social media (Facebook, etc.), digital safe schools, freedom of expression on-line, and human rights of students in digital settings		
Media and information literacy	A consultation, survey and whitepaper are prepared on European education, critical knowledge, skills and attitudes		DG2-Directorate of Democratic Citizenship and Participation, Education Department, Division on Education Practice and Capacity Building
Culture and digitisation	Annual Council of Europe Platform Exchanges on Culture and Digitisation will be held during the period 2016-2019 (the next annual Exchange will take place in October 2016 in Tallinn in the framework of the Estonian Presidency of the Council of Europe's Committee of Ministers), in particular to collect innovative digital cultural practices and potentials to orient policy making, including in view of meeting the challenges of inclusion Further policy guidelines will be prepared through multi-stakeholder consultation processes Good-practice collections will be assembled and published online		DG2-Directorate of Democratic Governance, Department on Democratic Institutions and Governance, Division on Culture and Democracy

Prioritising online safety and security for all			
Children's rights protection	Monitoring of and support to the implementation of the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention)		DG2-Directorate of Human Dignity and Equality, Equality and Human Dignity Department, Children's Rights Division
Action again cybercrime	Completion of the 3rd cycle of assessments on "sanctions and measures" in 2016, and the launch of further assessment cycles Develop solutions regarding criminal justice access to data on cloud servers and related issues of jurisdiction. Solutions may include a Protocol to the Budapest Convention on Cybercrime Support for more than100 capacity building activities per year in all regions of the world and ensure follow up to results of T-CY assessments Promote financial investigations and confiscation of crime proceeds on the Internet Establish a platform for public/private cooperation Promote implementation of Protocol to the Budapest Convention on Xenophobia and Racism (ETS 189)		DG1-Directorate of Information Society and Action Against Crime, Information Society Department, Cybercrime Division
Mass surveillance	Promotion of Convention 108 at the international level (Annual international Conference of Data Protection Authorities, Network of Francophone Data Protection Authorities) and assistance provided to interested countries (e.g. national initiatives addressing mass surveillance)		DG1-Directorate of Information Society and Action Against Crime, Information Society Department, Data Protection Unit
Extremism and radicalisation on the Internet	Develop a European strategy to counter extremism and radicalisation on the Internet, carried out in the framework of the Committee of Experts on Terrorism (CODEXTER)		DG1-Directorate of Information Society and Action Against Crime, Action Against Crime Department
Online abuse, such as cyber-stalking,	Monitoring the implementation on of the 'Istanbul Convention'		DG2-Directorate of Human Dignity and Equality, Equality

sexism and threats of sexual violence	The Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO) will carry out a first assessment of the implementation of the Istanbul Convention. More specifically, GREVIO will prepare a baseline questionnaire by March 2016 and subsequently examine reports submitted by the Parties in response to it. GREVIO may also carry out country visits before drawing up its evaluation reports Initial monitoring phase is expected to last for the whole duration of the 2016-2019 Internet Governance Strategy and possibly beyond		and Human Dignity Department, Violence Against Women Division
Respecting and protecting the human rights of everyone in the digital world			
Children's empowerment	As part of the Children's Rights Strategy (2016-2021): Creation and dissemination of tools to empower children, parents and educators in making full use of the potential of ICT and digital media Particular attention to empowering children in vulnerable situations, such as children with disabilities Development of guidance on rights-based parenting in the digital age Development of guidance for member States on an integrated approach to children's rights in the digital environment		DG2-Directorate of Human Dignity and Equality, Equality and Human Dignity Department, Children's Rights Division
Effective remedies online	Supporting the implementation of the Council of Europe Guide on human rights for Internet users by promoting the setting-up of a network of national institutions in line with the work of the European Committee on Legal Cooperation (CDCJ) on the effectiveness of online dispute resolution mechanisms having regard to Articles 6 and 13 of the European Convention on Human Rights		DG1-Directorate of Information Society and Action Against Crime, Information Society Department DG1-Directorate of Human Rights, Justice and Legal Cooperation Department, Legal Cooperation Division

Data protection and privacy on the Internet in Europe	Triennial reporting by the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD (subject to availability of findings of the evaluation and follow-up mechanism of the 'modernised' Convention 108 - not before 2018)		DG1-Directorate of Information Society and Action Against Crime, Information Society Department, Data Protection Unit
Internet intermediaries, and national law and practice in blocking, filtering and takedown of Internet content	Preparation of a new instrument on Internet intermediaries (Internet service providers and Internet platforms) Conclude and follow-up the comparative legal study on Internet blocking, filtering and takedown of content in the Council of Europe 47 member states		DG1-Directorate of Information Society and Action Against Crime, Information Society Department, Media and Internet Division (2016 – 2017)
Media and Internet freedom in Europe	Council of Europe platform for the safety and protection of journalism Reports of the Secretary General on the State of Democracy, Human Rights and the Rule of Law in Europe, with particular regard to freedom of expression on the Internet Recommendation of the Committee of Ministers on Internet freedom expected to be adopted in early 2016 coupled with its implementation by means of capacity building activities on Internet governance and the development of best practice Feasibility study on a possible standard-setting instrument on media coverage of elections, with particular regard to gender equality and the use of the Internet in elections Study of the human rights dimensions of automated data processing techniques (in particular algorithms) and their possible regulatory implications Reflection and dialogue on freedom of expression in the age of digital convergence, in particular on the future of journalism, news-making and media organisations, fear, self-censorship and ethics in journalism, the development of connected TV and		Directorate of Policy Planning DG1-Directorate of Information Society and Action Against Crime, Information Society Department, Media and Internet Division (2016 – 2017)

	challenges for pluralism and diversity of content and human rights, and the balancing the right to freedom of expression with the right to privacy in the context of removal of search results by search engines.		
Human rights and business on the Internet	Establish a platform between governments and major Internet companies and representative associations regarding the respect for human rights online Draft Recommendation of the Committee of Ministers on human rights and business expected to be adopted early 2016, coupled with Council of Europe side event at UN Forum on human rights and business (Geneva, November/December 2016 TBC)		DG1-Directorate of Information Society and Action Against Crime, Information Society Department DG1-Directorate of Human Rights, Human Rights Policy and Cooperation Department, Human Rights Intergovernmental Cooperation
Mobile health (mHealth) and electronic health (eHealth), including access to (quality) health and healthcare products, as well as the prevention of the illegal sale of drugs and counterfeit medicines	Revise 1997 recommendation on medical data to broaden its scope and address data protection challenges to health data Pompidou Group capacity building and training activities for law enforcement and judiciary, and provision of expertise and insight regarding online drug markets (detection and investigation including open source intel) and payment methods (cryptocurrencies) Pompidou Group expert group meeting on drug-related cybercrime (Strasbourg, November 2016 TBC) and other activities to promote international cooperation and sharing of good practices (including possible analysis of legal frameworks and model laws) Explore opportunities offered by the Internet for harm reduction, prevention and treatment, and collect and share best practices Follow-up to the international conference on emerging		DG1-Directorate of Information Society and Action Against Crime, Information Society Department, Data Protection Unit DG1-Directorate of Information Society and Action Against Crime, Pompidou Group DG1-Directorate of Human

	technologies and human rights		Rights, Human Rights Policy and Cooperation Department, Bioethics European Directorate for the Quality of Medicines and Healthcare, Biological Standardisation, OMCL Network and Healthcare Department , Pharmaceutical Care, Consumer Health Protection and Anti-Counterfeiting Section
Partnerships and synergies			
Cooperation with key stakeholders	Council of Europe support and participation in EuroDIG 2016 (Brussels, 9-10 June 2016) Council of Europe participation in IGF2016 (Mexico, dates TBC) Council of Europe participation in ICANN meetings (ICANN55-Marrakech, 6-11 March; ICANN56- Panama City,27-30 June; ICANN57-San Juan, 29 October-4 November		DG1-Directorate of Information Society and Action Against Crime, Information Society Department

APPENDIX VI

Composition of the
Committee of experts on media pluralism and transparency of media ownership - MSI-MED

Composition du
Comité d'experts sur le pluralisme des médias et la transparence de leur propriété – MSI-MED

MEMBER STATES REPRESENTATIVES

1. Ms Helena Mandić - Director of Broadcasting - Communications Regulatory Agency - Bosnia and Herzegovina
2. Mr Nol Reijnders - Senior Adviser - Department for Media, Literature, Libraries - Ministry of Culture, Education and Science - The Netherlands
3. Ms Maria Donde - International Policy Manager in Ofcom – United Kingdom
4. Ms Maja Zaric - Media Advisor - Media Department - Ministry of Culture and Information - Republic of Serbia
5. Mr Evangelos Valmas - Head of Department for Audiovisual Media and Archives - Secretariat General of Information and Communication - Greece
6. Ms Natalie Fercher - Expert on Media and Communication Law - Department of Media Law and Coordination Information Society - Federal Chancellery - Austria
7. Mr Gudbrand Guthus - Director Licensing and Supervision Department - Norwegian Media Authority – Norway

INDEPENDENT EXPERTS

1. Damian Tambini - Associate Professor - Director of the Media Policy Project - Programme Director: MSc Media & Communications (Governance) -London School of Economics
2. Mr Tarlach McGonagle - Senior Researcher and Lecturer, Institute for Information Law (IViR) - University of Amsterdam
3. Ms Elda Brogi - Scientific Coordinator - Centre for Media Pluralism and Media Freedom - Robert Schuman Centre for Advanced Studies - European University Institute
4. Ms Helena Sousa - Associate Professor - Department of Communications Sciences -University of Minho
5. Mr Josef Trappel - Professor for media policy and media economics - Head of the Department of Communication Research at the University of Salzburg
6. Mr Pierre François Docquir - Senior Legal Officer - ARTICLE 19

REPRESENTANTS DES ETATS MEMBRES

1. *Mme Helena Mandić - Directrice de la radiodiffusion - Autorité de régulations des communications - Bosnie-Herzégovine*
2. *M Nol Reijnders - Conseiller principal - Service des médias, de la littérature et des bibliothèques - Ministère de la culture, de l'éducation et des sciences - Pays-Bas*
3. *Mme Maria Donde - Gestionnaire des politiques internationales de l'Ofcom - Royaume-Uni*
4. *Mme Maja Zaric - Conseillère des médias - Service des médias - Ministère de la culture et de l'information - République de Serbie*
5. *M Evangelos Valmas - Chef du service des médias et archives audio-visuels - Secrétariat général de l'information et de la communication - Grèce*
6. *Mme Natalie Fercher - Experte en droit des médias et de la communication - Service du droit des médias et coordination de société de l'information - Chancellerie fédérale – Autriche*
7. *M Gudbrand Guthus - Directeur du service des licences et de la surveillance - Autorité des médias de Norvège – Norvège*

EXPERTS INDÉPENDANTS

1. *M Damian Tambini – Professeur agrégé - Directeur du projet de politiques des médias - Directeur du programme MSc Media & Communications – London School of Economics*
2. *M Tarlach McGonagle - Chercheur principal et conférencier à l'Institut pour le droit de l'information (IViR) - Université d'Amsterdam*
3. *Mme Elda Brogi - Coordinatrice scientifique - Centre pour le pluralisme et la liberté des médias - Centre d'études avancées Robert Schuman - Institut de l'université européenne*
4. *Mme Helena Sousa - Professeur agrégé - Service des sciences de la communication - Université de Minho*
5. *M Josef Trappel - Professeur en politiques des médias et économie des médias - Chef du service de recherche en communications de l'Université de Salzbourg*
6. *M Pierre François Docquir - Juriste principal - ARTICLE 19*

APPENDIX VII

Composition of the
Committee of experts on Internet intermediaries - MSI-NET

Composition du Comité d'experts sur les intermédiaires internet - MSI-NET

MEMBER STATES REPRESENTATIVES

1. Ms Karmen Turk – Trinity Tallinn – Estonia

2. Mr Bertrand de la Chapelle – Co-founder and Director of the Internet & Jurisdiction Project, member of ICANN Board – France

3. Ms Sabine Maass – Head of Division 'Legal framework for digital services, media industry', Federal Ministry for Economic Affairs and Energy – Germany

4. Mr Pēteris Podvinskis – Ministry of Foreign Affair International Organisations, Public Policy related to Internet Latvia

5. Mr Arseny Nedyak – Deputy Director, Department of media state policy, Ministry of telecommunication – Russian Federation

6. Ms Tanja Kerševana Smokvina – Principal Advisor to Director General, Agency for Communication Networks and Services – Slovenia

7. Mr Thomas Schneider – Deputy Director of International Affairs, International Information Society Coordinator, Federal Department of the Environment, Transport, Energy and Communication DETEC, Federal Office of Communications (OFCOM) – Switzerland

INDEPENDENT EXPERTS

1. Ms Julia Hornle – Professor of Internet Law, Queen Mary University of London

2. Mr Matthias Kettemann – Postdoc Fellow, Cluster of Excellence "Normative Orders" University of Frankfurt/Main, Germany – Austria

3. Mr Wolfgang Schulz – Professor, Faculty of Law at the University of Hamburg and the Hans-Bredow-Institut

4. Ms Sophie Stalla-Bourdillon – Associate Professor in Information Technology / Intellectual Property Law, Director of ILAWS, Southampton Law School at the University of Southampton

5. Mr Dirk Voorhoof – Professor at Ghent University, member of the CMPF Scientific Committee, Centre for Media Pluralism and Press Freedom

6. Mr Ben Wagner – Director of the Centre for Internet & Human Rights at European University Viadrina.

REPRESENTANTS DES ETATS MEMBRES

1. *Mme Karmen Turk – Trinity Tallinn – Estonie*

2. M Bertrand de la Chapelle – Co-fondateur et Directeur du Projet Internet & Jurisdiction, membre du board des directeurs de l'ICANN – France

3. Mme Sabine Maass – Chef de la division « Cadre juridique pour les services numériques, l'industrie des médias », Ministère Fédéral de l'Economie et de l'Energie - Allemagne

4. M Pēteris Podvinskis – Ministère des affaires étrangères, des Organisations Internationales, des Politiques publiques dans le domaine de l'Internet – Lettonie

5. M Arseny Nedyak – Directeur adjoint, Service des politiques nationales des médias, Ministère de la télécommunication – Fédération de Russie

6. Mme Tanja Kerševana Smokvina - Conseillère principale au directeur général - L'Agence pour les réseaux et services de communication - Slovénie

7. M Thomas Schneider – Directeur adjoint des affaires internationales, Coordinateur de la société d'information internationale, Service fédéral de l'environnement, transport, énergie et communication DETEC, Office fédéral des communications (OFCOM) – Suisse

EXPERTS INDÉPENDANTS

1. Mme Julia Hornle – Professeur des lois dans le domaine d'Internet, Queen Mary University of London

2. M Matthias Kettemann – Postdoc Fellow, Cluster of Excellence "Normative Orders" Université de Francfort-sur-le-Main, Allemagne – Autriche

3. M Wolfgang Schulz – Professeur, Faculté de droit de l'Université de Hambourg et l'Institut de Hans-Bredow

4. Mme Sophie Stalla-Bourdillon – Professeur agrégée en technologie d'information / droit de la propriété intellectuelle, Directrice de ILAWS, Faculté de droit de Southampton de l'université de Southampton

5. M Dirk Voorhoof – Professeur à l'université de Ghent, membre du comité scientifique CMPF, Centre pour le pluralisme des médias et la liberté de la presse

6. M Ben Wagner – Directeur du Centre pour Internet & droits de l'Homme de l'université européenne Viadrina.