24 March, 2015

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

Introduction

Access is a global organization dedicated to defending and extending the digital rights of users at risk around the world. Access works through its Policy, Technology, and Advocacy teams to achieve this mission. Access provides thought leadership and policy recommendations to the public and private sectors to ensure the internet's continued openness and universality and wields an action-focused global community of nearly half a million users from more than 185 countries. Access also operates a 24/7 digital security helpline that provides real-time direct technical assistance to users around the world. Access is non-partisan and not affiliated with any country, corporation, or religion.

Access welcomes the opportunity given by the Council of Europe to provide feedback to the draft recommendation by the Committee of Ministers to its member states on Internet freedom. Our comments and suggestions focus on access to remedy, transparency, the openness of the internet and the rights to privacy and data protection.

Suggestions can be found marked **in bold** and ~~strike-through~~ directly in the text and comments are indicated in a box under the relevant sections.

Feedback on the report

1. The European Convention on Human Rights (hereinafter the ECHR) applies without any distinction to the physical world and to the Internet. The Council of Europe member States have both negative and positive obligations to protect and promote human rights and fundamental freedoms on the Internet.

2. The Council of Europe~~'s~~ member States' understanding of Internet freedom should not be bound by different cultural or political approaches or sensitivities but should instead be construed as the exercise and enjoyment on the Internet of the fundamental rights and freedoms which are enshrined in the ECHR. Internet freedom should be considered as part of an affirmative vision and a proactive role of the implementation of the ECHR and other Council of Europe standards on the Internet by Council of Europe member states.

3. Internet governance arrangements, whether national, regional or global, must build on this ~~notion~~ **definition** of Internet freedom. States have rights and responsibilities with regard to international Internet-related policy. In the exercise of their sovereignty rights, states ~~should~~ **must**, subject to international law, refrain from any action that would directly or indirectly harm persons or entities **inside and** outside of their territorial jurisdiction. Any national decision or action amounting to a restriction of fundamental rights ~~should~~ **must** comply with international obligations**,** ~~and in particular~~ be based on law, necessary in a democratic society**,** and fully respect the principles of proportionality and **guarantee access to remedy and** the right **to fair trial** ~~of~~ and **to an** independent appeal with due process safeguards.

4. As part of their duty to ~~secure~~ **protect** the rights and freedoms enshrined in the ECHR, States should create an enabling environment for Internet freedom. In this regard States should not only fulfil a range of positive and negative obligations with regard to these rights and freedoms but also 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 greater 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 conceptualised 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 has a key role to play in promoting Internet freedom in Europe **and beyond**. 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 polic**ies**~~y~~.

7. The Committee of Ministers recommends to member states to:

- periodically evaluate the implementation **and respect** 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 **on an equal footing** of all stakeholders from private sector, civil society**, academia** and technology experts in their evaluation of the state of Internet freedom and development of national reports;

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

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

- ensure **the respect** of these standards ~~on~~ **by** private companies under their jurisdiction or effective control, and require increasingly refined **reporting** by companies on their compliance;

8. The Committee of Ministers also invites the Secretary General of the Council of Europe to elaborate an annual report which provides an overview of Internet freedom challenges in Council of Europe member states.

INTERNET FREEDOM INDICATORS

These indicators focus on the right to freedom of expression, the right to freedom of assembly and association and the right to private life. They 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. They are not designed to rate the levels of Internet freedom or as a means of comparing countries to each other.

I- An enabling environment for Internet freedom

1. Constitution**s**~~al or~~**and** any other national law**s** guarantee the protection of human rights and fundamental freedoms on the Internet in full compliance with the ECHR.

2. The State does not interfere with the exercise of human rights and fundamental freedoms on the Internet and protects these rights from interference by non-state actors.

3. The State creates an enabling environment for the exercise of human rights and fundamental freedoms on the Internet.

4. Laws and policies relating to the Internet are assessed at the **draft** stage ~~of~~ **and during** their development with regard to negative impact**(s)** that their implementation may have on the exercise of human rights and fundamental freedoms.

5. Laws and policies relating to the Internet are developed by State authorities in an ~~open~~ **inclusive and transparent** process which enables the participation of all stakeholders, **including the private sector, civil society, academia and technology experts.**

6. Any state body which has regulatory or other competence over Internet matters **must** carr**y**~~ies~~ its activities independently of political or commercial interference, in a transparent **manner**~~way~~ and protect~~s~~ and promote~~s~~ Internet freedom.

7. The State provides digital literacy programmes for users to foster their ability to make informed decisions and give~~s~~ access to digital education and knowledge in order to exercise rights and freedoms on the Internet. **The state promotes the use and development of open source sofware.** The state promotes access to education, cultural, scientific, scholarly and other content in official languages.

8. The State promotes **a decentralised and multi-stakeholder approach to Internet regulation, in accordance with the rule of law** ~~Internet self regulation the development and existence of ethical standards for Internet users~~.

II. The right to freedom of expression

1. Freedom to connect

1.1. There are no infrastructural limitations or financial barriers which negatively impact the availability, accessibility and affordability of Internet access for all groups of population without any discrimination.

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

1.3. The State takes–measures to ensure that **unrestricted access to the** Internet ~~access~~ is available and affordable to those in low income, in rural or geographically remote areas and those with special needs such as **persons with disabilities**. ~~disabled persons~~.

1.4. The State recognises in law and in practice that disconnection of individuals from Internet access is a disproportionate restriction on the right to freedom of expression. Any disconnection measure is taken only if safeguards for freedom of expression are in place**,** in compliance with Article 10 of the ECHR**,** and the right to due process and **access to remedy is ensured** ~~including a right to be heard and/or a right of appeal~~.

1.5. The law does not impose blanket prohibitions on **access to the** Internet ~~access~~. State polic**ies**~~y~~ and legislation ensure that general **access to the** Internet ~~access~~ is maintained at

all times notwithstanding political difficulty, opposition or turmoil, by all Internet service providers of all forms of infrastructure through any technology.

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

2.1. The State or any other actor**, public or private,** does not block or otherwise restrict access to **the Internet** and**/or the** usage of Internet platforms (social media, social networking, blogging or any other websites) or ICTs tools (instant messaging or other applications) **offered through an Internet access service**.

2.2. The State does not impose removal of Internet content by Internet platforms prior or after its publication **without a court order**.

2.3. Any decision to block or otherwise restrict access to Internet platforms, ICTs tools or to remove Internet content is taken by a court ~~or an independent administrative authority whose decisions are subject to judicial review~~.

2.4. A **necessary** blocking, filtering or content-removal decision ~~is as~~ **must be transparent,** targeted and ~~as~~ specific ~~as possible~~**.** ~~based on a~~**A**n assessment **evaluating the** ~~of its~~ effectiveness~~,~~ ~~risks of over-blocking~~ **and proportionality of the measure must be conducted, in particular to determine** ~~(~~whether it leads 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.

2.5. Internet service providers manage Internet traffic in a transparent**, necessary and proportionate** manner**,** ~~and~~ without discrimination on the basis of sender, receiver, content, application, **localisation**, service or device **used**.

2.6. 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 ~~access~~ **receive** and impart content.

2.7. The State provides information to the public about any restrictions, such as lists of blocked websites, together with details of the **legal basis,** necessity**,** ~~and~~ justification **and court order authorising** ~~for~~ the blocking or restriction.

3. Freedom of the media

3.1. The editorial independence of news and media outlets operating on the Internet is guaranteed in regulation/ policy and in practice. They are not subjected to pressure by political or commercial actors**, public or private,** to include or exclude information from their reporting or to follow a particular editorial direction.

3.2. News and media outlets operating on the Internet and new media actors, including blogging websites are not required obtain permission or licence from the government or state authorities which goes beyond business registration in order to be allowed to operate or blog.

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.

3.4. The confidentiality of journalists and other media actors' sources is guaranteed by law. Their activities on the Internet are not subjected to surveillance.

3.5. Websites of news and media outlets operating on the Internet and websites of new media actors are not subjected to cyber attacks or other action disrupting their functioning (e.g. denial of service attacks).

3.6. Press, radio, broadcasters and new media content is not subjected to discrimination through traffic management.

4. Legality, legitimacy and proportionality of restrictions

4.1. Any restriction of the right to freedom of expression on the Internet is in strict compliance with the requirements of Article 10 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 10 of the ECHR;

- is necessary in **a** democratic society and ~~therefore~~ ~~proportional~~ **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 expression 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 expression.

4.2. The State ~~does not~~ **must 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 criminal sanctions, excessive fines or disproportionate awards of damages or legal costs.

4.3. Laws addressing hate speech or protecting public order, ~~public morals~~, national security or official secrecy do not inhibit public debate ~~about issues of public concern~~. Such laws impose restrictions on 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 proportional sanctions.

III. The right to freedom of assembly and association

1. Individuals are free to use Internet platforms, such social media and other ICTs, whether on fixed or mobile devices to establish associations, to determine the objectives of such

associations and to carry out activities within the limits provided for by laws that comply with international standards.

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

3. Individuals are free to use Internet platforms, such social media and other ICTs and applications, whether on fixed or mobile devices, to organise themselves for purposes of peaceful assembly.

4. The state does not block or otherwise restrict Internet platforms, such as social media or other ICTs in the context of the exercise of the right to peaceful assembly.

5. 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 strict 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;

- is necessary in **a** democratic society and ~~therefore proportional~~ **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**.

IV. The right to a private life

1. Personal data protection

1.1. The law guarantees that all personal data ~~is~~ **are** protected in strict compliance with Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108).

1.2. The law is sufficiently clear and precise with regard to the conditions for collecting, storing and processing personal data, including clear and ~~unambiguous~~ **explicit** consent of the data subject. The law defines the duties of public and private entities with regard to collecting, storing and processing personal data ~~personal data~~.

1.3. With regard to intermediaries and data profiling (personal data processing techniques that **collect and use information about** ~~apply a profile to~~ an individual in order to **identify patterns and make assumptions about** ~~take decisions for purposes of analysing or predicting~~ his or her personal preferences, future behaviour and attitudes):

- the law or policy framework is sufficiently **accessible,** clear and precise with regard to the conditions for the collection and processing of personal data in the context of data profiling. Such conditions include:
- **lawfulness of collection and processing based on explicit consent from individuals, including in case of further processing of data;**
- individual's right to access, to rectification, to object and to erasure of his or her personal data;
- right to remedy;
- data quality **and security;**
- and information to Internet users **regarding the purpose and use of the personal data collected and processed**.
- and no individual shall be subject to a decision significantly affecting him/her based solely on the automated processing of data without having their views taken into consideration

- ~~there are effective tools~~ **and processes** ~~for Internet users to consent to, object to or withdraw from profiling and to secure correction, deletion or blocking of their personal data.~~

Comments

Suggestions in this section are based on the modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data - *Convention 108* - as adopted by the 29th Plenary meeting on December 2012: http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD%282012%2904Rev4_E_Convention%20108%20modernised%20version.pdf

2. Freedom from surveillance

2.1. **Suspicionless** surveillance on the Internet which consists of bulk access to, collection and retention of communications data (content and metadata including information on individuals, their location and online activities) ~~is done in accordance with the law which is accessible, clear~~**,** ~~and precise and foreseeable~~ **is inherently disproportionate and as such in violation of the principles of necessity and proportionality and therefore a violation of human rights.**

2.2. The law contains ~~minimum~~ safeguards for the exercise of discretion by public authorities and ~~thus~~ defines with sufficient clarity and precision:

- the offences and activities in relation to which **targeted** surveillance **on the basis of suspicion** may be ordered;

- the procedures and relevant authorities by which targeted surveillance is allowed;

- the ~~categories of~~ individuals who may be subjected to surveillance **on the basis of suspicion**;

- time limitations for carrying out **targeted** surveillance;

- the procedures for examining, using and storing the data obtained from **targeted** surveillance;

- the **rules and legal basis authorising the** ~~precautions to be taken when~~ communicati**on**~~ng~~ **of** the data **acquired through targeted surveillance** to other parties, **as well as the measures applying during the communication to ensure data security**;

- the rules on the destruction and erasure of data obtained from **targeted** surveillance;

- the bodies responsible for ~~supervising~~ **overseeing** the use of surveillance powers.

2.3. Any **targeted** surveillance measure pursues a legitimate aim as exhaustively enumerated in Article 8 of the ECHR.

2.4. Any **targeted** surveillance measure responds to a **necessary** pressing social need in a democratic society and ~~thus~~ is proportionate. **If a less intrusive measure is capable of achieving the same goal the least restrictive measure is applied.**

2.5. Any **targeted** surveillance measure is subject to a~~n effective~~ **judicial order and judicial** control ~~assured by the judiciary or another state body~~ offering the best guarantees of independence from the authorities carrying surveillance, impartiality and a proper procedure.

2.6. There are independent public oversight mechanisms (including Parliamentary oversight) to avoid abuse of power and arbitrariness and to ensure transparency and accountability of surveillance on the Internet.

2.7. The State does not prohibit anonymity**, pseudonymity** and confidentiality of 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.

V - Internet intermediaries

1. Internet intermediaries do not restrict the human rights and fundamental freedoms of their users. The intermediaries' policies comply with international human rights law. They assess the impact of their services and technologies on Internet freedom **and fundamental rights**.

2. The State does not require Internet access ~~and service~~ providers, **Internet service providers, and** Internet platforms such as social media or networks to prevent access to or remove content unless this is in strict compliance with Article 10 of the ECHR **and requested by a court order**. **Request for such restrictions of content must be clear, unambiguous, in line with due process, and respect the principles of necessity and proportionality.** Internet intermediaries are not coerced or pressured to follow a particular editorial direction, policy or political party line.

3. The State does not require disclosure of personal data of Internet users unless this is in strict compliance with Article 8 of the ECHR and Convention 108 **and requested by a court order**.

4. Internet intermediaries are not obliged to monitor content on the Internet to which they give access, transmit or store. They are not obliged to search for facts potentially relating to illegal activity.

5. Internet intermediaries are held liable for content uploaded onto their systems by Internet users or other parties only when they do not act expeditiously to remove or disable access to information or services **as requested by a court order** ~~as soon as they become aware of their illegal nature~~.

6. Internet intermediaries inform Internet users about restrictive measures taken and put in place **effective** procedures **to ensure** ~~for~~ users**' right to redress** ~~to appeal~~.

7. State has an obligation to ensure that general terms and conditions of private companies that are not in accordance with international human rights standards must be held null and void.

Comments:

Suggestions in this sections are based on the Council of Europe's issue paper on "The rule of law on the Internet and in the wider digital world".

VI. Remedies

1. The State ensures that individuals have access to ~~a~~ judicial ~~or administrative process~~ **procedures** that can impartially decide on their claims concerning violations of human rights online in compliance with Article 6 of the ECHR. **These processes are clear and unambiguous.**

2. The State provides for the right to an–effective remedy in compliance with Article 13 of the ECHR.

3. The United Nations Guiding Principles on Business and Human Rights (UNGPs) likewise affirm that victims must have access to an effective remedy for abuses. In accordance with Guiding Principle 26, the State takes appropriate steps to investigate, punish, and redress business-related human rights abuses when they occur. This State obligation applies to the activities of businesses within the jurisdiction or effective control of the State, and their subsidiaries, and extends to victims regardless of where they are located or where the harm took place. As communications and information seamlessly cross borders, so too must protections for users.

4. The State promotes the implementation of the UNGPs within its national context. The State has produced or is in the process of producing both a National Baseline Assessment (NBA) of current State implementation of the UNGPs and an actual National Action Plan (NAP) on business and human rights. The State follows the NBA and NAP with monitoring and review of NAPs once they are developed in order to optimize their value within and between countries as a means for improving governance, regulation, and, ultimately, respect for human rights.

5. The State provides for both civil and criminal accountability of businesses for their direct involvement or complicity in abuses of the rights listed in this document, including for business' involvement in such abuses both within and beyond the State's territorial jurisdiction.

6. The State has reduced and eliminated, or is in the process of reducing and eliminating, the legal, financial, procedural, and other practical barriers that individuals encounter in seeking an effective remedy. In particular, the State ensures that barriers to information and accountability on surveillance, including national security exemptions, state secret claims, and forms of immunity for business enterprises, are scrutinised for their compliance with fundamental rights, in particular the principles of due process, necessity, and proportionality as explained above.

Comments:

Suggestions in this section are made in order to enable an effective implementation of the ECHR online. They follow recommendations for efficient implementation of remedies, from the United Nations Guiding principles on Business and Human Rights and the International Corporate Accountability Roundtable (see here and here).

For more information, please contact Raegan MacDonald, European Policy Manager, raegan[at]accessnow[dot]org or by phone at +32 227 425 74.