

**Committee of experts on Internet intermediaries**

**(MSI-NET)**

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

**7 March 2016**

**MSI-NET(2016)03**

**MSI-NET 1<sup>ST</sup> MEETING**  
**17-18 March 2016 (9:30-17:30)**  
**Strasbourg, Palais de l'Europe (Room 7)**

**Roles and responsibilities of Internet intermediaries**  
**Issue mapping non-paper prepared by the Secretariat**

This non-paper has been prepared by the Secretariat to facilitate discussions of the MSI-NET at its first meeting. The issues and questions identified here are not exclusive and are open to further elaboration during meeting discussions. Together with references to documents and reading materials they are aimed at guiding reflections and preparing discussions. The indicated times are of an advisory nature.

**1) Definition of Intermediaries** (60 min)

- What is an Internet intermediary? Access providers, hosting providers, both, applications, connected-economy operators, any others? How to define intermediaries, should we use a broad or strict definition? Are there any clear dividing lines?
- How to categorise intermediaries? Should we treat them differently in the recommendation?

\* Short presentation by European Audiovisual Observatory.

*Relevant documents*

Report "[Fostering Freedom Online: The Role of Internet Intermediaries](#)" (UNESCO)  
[OECD The economic and social role of Internet intermediaries](#)

## **2) Human rights responsibilities<sup>1</sup>** (90 min)

- What are the human rights implications of intermediaries' actions?
- What are their responsibilities according to the ECtHR, international standards?
- How do these stand vis-à-vis states' obligations to secure human rights?
- How to address them in a recommendation?
- Human rights impact assessment.
- Co-operation between States and intermediaries: challenges and practical solutions.

\* Presentation by EuroISPA

Short presentation by Ranking Digital Rights

*Relevant documents*

[UN Guiding Principles on Business and Human Rights](#)

[Recommendation of the Committee of Ministers to member States on Human Rights and business](#)

[ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights](#)

[Human rights guidelines for Internet service providers \(Council of Europe/EuroISPA\)](#)

[Recommendation CM/Rec\(2014\)6 of the Committee of Ministers to member States on a Guide to human rights for Internet users](#)

[Recommendation CM/Rec\(2012\)3 of the Committee of Ministers to member States on the protection of human rights with regard to search engines](#)

[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](#)

[Judgment of the ECtHR K.U. v. Finland \(case no. 2872/02\).](#)

### 2.1 Freedom of expression (90 min)

- Role of Internet intermediaries in implementing limitations of access to the Internet.
- Restriction of content: blocking, filtering and takedown. What kind of content can be removed? How to define illegal content? What happens with content that may "offend, shock or disturb"? How to avoid over-blocking?
- Are intermediaries acting as gatekeepers and assuming a "judge" role?
- Are measures foreseeable? Terms of service: need for availability and clarity (also when they are modified).

---

<sup>1</sup> Only two sub-sections have been created dealing with freedom of expression and privacy and data protection, this does not mean that these are the only human rights affected. The activities of intermediaries also have an impact in the exercise of other rights and freedoms such as the freedom of association or assembly, for example, or participation in a democratic society.

- How can we ensure compliance with article 10 ECHR?
- Role of intermediaries in the creation of a public sphere.

*Relevant documents*

[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](#)

[Recommendation CM/Rec\(2016\)1 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](#)

[Judgment of the ECtHR Yildirim v. Turkey \(case no. 3111/10\)](#)

[Judgment of the ECtHR Cengiz and Others v. Turkey \(cases nos. 48226/10 and 14027/11\)](#)

[Ways to tackle online hateful content proposed by the German Task Force against illegal online hate speech](#)

## 2.2 Privacy/Data protection (90 min)

- Are privacy policies of Internet intermediaries clear and accessible?
- Are users aware of what can be done with their data/also when it could be transferred to third countries?
- Are users able to have access to the information processed and are able to ensure its correction or deletion?
- What are the processes to give information about users to third parties (law enforcement/private parties)? Is a court order necessary?
- How can we ensure compliance with article 8 of ECHR and the data protection principles of Convention 108?

\* Short presentation by the Data Protection Unit of the Council of Europe.

*Relevant documents*

[Handbook on European data protection law](#)

[The right to privacy in the digital age](#) (Report of the Office of the United Nations High Commissioner for Human Rights)

[Judgment of the CJEU, Maximilian Schrems v Data Protection Commissioner, case C-362/14.](#)

[Judgment of the CJEU, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others \(C-293/12\) and Kärntner Landesregierung and Others\(C-594/12\)](#)

### **3) Intermediary liability regimes** (90 min)

- Are notice-and-take-down systems enough? How do they work in practice? What are the main loopholes in terms of ensuring human rights protection?
  - Should some Internet intermediaries have a more active role in the fight against illegal content?
  - Do intermediaries play a role in content production and dissemination similar to publishers? Do they have an editorial role? How to distinguish it from a technical intermediary role?
  - How do knowledge-based liability regimes for illegal content operate?
- \* Short presentation by Article 19 of the Manila Principles on Intermediary Liability.

#### *Relevant documents*

[Recommendation CM/Rec\(2011\)7 of the Committee of Ministers to member states on a new notion of media](#)

Report "[Internet intermediaries: Dilemma of Liability](#)" (Article 19)

["Manila Principles on Intermediary Liability"](#) (different civil society organisations)

[Cyberhate: an issue of continued concern for the Council of Europe's Anti-Racism Commission](#)

[Governance of Online Intermediaries: Observations from a Series of National Case Studies](#)

[Judgment of the ECtHR Delfi AS v. Estonia \(case no. 64569/09\) \(2015\)](#)

[Judgment of the ECtHR Magyar Tartalomszolgáltatók Egyesülete and Index.hu ZRT v. Hungary \(case no. 22947/13\)](#)

[Offensive Online Comments - New ECtHR Judgment – commentary by Dirk Voorhoof and Eva Lievens](#)

### **4) Procedural guarantees** (90 min)

- Transparency and accountability;
- Availability of mechanisms to report illegal content;
- Process for third party claims;
- Notification of restrictions;
- Alternative dispute resolution;
- Judicial remedies;
- Do intermediaries have the opportunity to react against State orders that may endanger human rights?

*Relevant documents*

[Ranking Digital Rights](#)

### **5) Applicable law and jurisdiction** (60 min)

- Which laws apply to intermediaries which are incorporated in one country and offer their services in other countries? How does the location of data stored in different countries affect the applicable law issues?
- What happens when various laws could be applied that do not have the same standards of protection of freedom of expression or data protection?
- Which jurisdiction is competent to solve a controversy in these cases?
- How can court judgments be effectively enforced if the Internet intermediary is located in another country or it is not clear where the data is located? How to avoid legal uncertainty for users but also Internet intermediaries?

\* Short presentation by Cybercrime Division of the Council of Europe (work of the Cloud Evidence Group)

*Relevant documents*

[Criminal justice access to data in the cloud: challenges](#)

[Welcome to the Jungle: the Liability of Internet Intermediaries for Privacy Violations in Europe](#)

[Judgment of the CJEU Google Spain SL, Google Inc. v Agencia Española de Protección de Datos \(AEPD\), Mario Costeja González \(case C-131/12\)](#)

### **6) Human rights aspects of algorithms** (120 min)

- Definition of algorithms, what are their functions? What decisions do they make typically? What are the decision-making criteria built in algorithms? Are these criteria fair and non-discriminatory?
- How do algorithmic decisions impact the exercise and enjoyment of human rights and the public interest? What is the significance of errors in algorithmic decisions?
- Transparency of algorithmic decision-making – do people who are affected by such decisions have information about their consequences?
- Should we focus on specific algorithms, e.g. predictive policing (how can it be reconciled with basic criminal law principles like presumption of innocence or due process)? E.g. how can we ensure the right to receive information and media pluralism against the danger of an information bubble?
- Algorithmic power accountability - how to hold decisions made by algorithms accountable?

- How can we ensure the effectiveness of the principle of non-discrimination on the decisions taken by algorithms?
- How is algorithmic power used by governments and companies? What does it mean for society? While legislative regulation of algorithms takes time what mechanism should there be in place to check and balance algorithmic power.

*Relevant documents*

[Recommendation CM/Rec\(2010\)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling](#)

Report "[The Ethics of Algorithms: from radical content to self-driving cars](#)" (Center for Internet and Human Rights)

[Algorithmic Power and Accountability in Black Box Platforms](#)

[France: An Algorithmic Power](#)

[Predictive Policing. Can data analysis help the police to be in the right place at the right time?](#)