

18 May 2016

MSI-NET(2016)05

Draft Recommendation CM/Rec(201x)xx of the Committee of Ministers to member States on Internet intermediaries

DRAFT STRUCTURE 1.0 (18 MAY 2017)

Rapporteur: Matthias C. Kettemann

1. [definition of intermediaries: functional, broad approach – user realities and HR impact matters]¹
2. [Freedom of expression is the key enabling right of the Internet: Article 10 ECHR and Article 19 ICCPR, offline just as online; includes content, dissemination, hosting]
3. [Intermediaries essential and critical for exercising FoE in the information society: enabling, facilitating, controlling and influencing access to and availability of content; but also other rights: privacy, data protection ...]
4. [human rights law targeted at states, but corporate social responsibility and HR obligations for private actors as well]
5. [Challenge # 1: Intermediaries can endanger FoE – by themselves [for commercial reasons] or under pressure from states; HR law sets limits]
6. [Challenge # 2: chilling effects of overextending intermediary liability, especially with regard to defamation, copyright and IP law]

¹ [Internal note: This one seems very useful: "services that are: (a) "in between" content and users; (b) show structural relevance to public communication (i.e. are not merely private); and (c) are not traditional journalistic-editorial ("media") services." (Gasser/Schulz, Governance Of Online Intermediaries: Observations From A Series Of National Case Studies, Network of Centers Online Intermediaries Research Project: Synthesis, https://publixphere.net/i/noc/page/NoC_Online_Intermediaries_Research_Project_Synthesis).

7. [Challenges # 3: difficulty of operating under different legal frameworks: intersection of international law, European law and national public law]
8. [Challenge #4: privatizing public social communicative spaces and monetarizing the aggregation and articulation of opinions; problem of market domination]
9. [Solution # 1 : increasing 'normative literacy', providing readable terms of service, attractivizing HR-sensitive freedom of expression 'management' frameworks; importance of an enabling environment for both intermediaries and users]
10. [Solution #2: maximizing human rights protection; minimizing human rights interferences: ensuring maximum of accountability of intermediaries to their users especially regarding the criteria of selecting, aggregating and presenting information, if applicable; minimizing informal governmental interference; making governmental requests plainly visible in disaggregated form]
11. [Solution #3: reducing chilling effects and legal fragmentation by ensuring development of common standards, judicial cooperation and dialogue through transnational due process frameworks]
12. [Solution #4: importance of allowing self-regulation frameworks, combined with procedural guarantees and recourse to courts]
13. [Solution #5: identifying best practices and drawing conclusions from them]
14. [The Committee of Ministers recalls Article 1 of the Statute of the Council of Europe (ETS No. 1) and relevant Council of Europe instruments, [including relevant documents such as Recommendation [CM/Rec\(2008\)6](#) on measures to promote the respect for freedom of expression and information with regard to Internet filters, the Human rights guidelines for Internet service providers (H/Inf (2008) 9), the Declaration of the Committee of Ministers on network neutrality (29 September 2010), the Declaration by the Committee of Ministers on Internet governance principles (21 September 2011) and Recommendation [CM/Rec\(2014\)6](#) to member States on a Guide to human rights for Internet users)]
15. [Therefore, the Committee of Ministers, under the terms of Article 15.b of the Statute of the Council of Europe, recommends that member States, when developing and implementing Internet-related policies at the national and regional level and within the international community
 - ensure that these protect and promote all human rights, including the right to private life and the right to freedom of expression,
 - promote best practices regarding the role of Internet intermediaries,
 - take all necessary measures, in co-operation with all relevant stakeholders, to ensure that national, regional and international law applicable for Internet intermediaries is in full compliance with Articles 8 and 10 of the Convention,
 - support the evolution of a legal framework, at the appropriate level, that maximizes user rights, minimizes administrative burdens put on Internet intermediaries, allows for robust self-regulatory frameworks, and contributes to the emergence of transnational judicial dialogue on due process,

- take all the necessary measures, in co-operation with all relevant stakeholders, to ensure that Internet intermediaries can fulfill their role in the information society without being made complicit in human rights violations,
- in doing so, adopt national and contribute to regional and international policy frameworks with due regard to the Guidelines on Internet Intermediaries set out in the appendix to this recommendation;
- promote these guidelines in other international and regional forums that deal with Internet intermediaries.]

Appendix to Recommendation: Guidelines on Internet Intermediaries

1. [General principles]

- a. [Definition: functional, broad approach – user realities and HR impact matters; relation to EU law, new E-Commerce-Directive]
- b. [relevant distinction between commercial and non-commercial intermediaries? between those 'making available' and 'hosting' information?]
- c. [Role of intermediaries in the information society –framing the conditions under which information is sought, distributed and received; selecting, aggregating and presenting information under certain conditions]
- d. [These *conditions* – framed by national, European and international law, and by terms of service, soft law and code – are at issue here.]
- e. [all human rights that apply offline also apply online; with regard to intermediaries special emphasis is put on FoE, privacy, data protection]
- f. [overcoming the illusion of automation in decisions over content: norms matter]
- g. [overcoming the challenge of conflicts of laws and jurisdictions]
- h. [goal should not be the creation of new standards but rather the application of existing ones, combined with lessons drawn from best practices]
- i. [shared but differentiated responsibility of all stakeholders in *four* dimension of a matrix: state-user, state-intermediary, intermediary-user, user-user conflicts]
- j. [mix of self-regulation with judicial redress mechanisms, state regulation and transnational judicial dialogue is best suited to regulate intermediaries]

2. [States, intermediaries and human rights]

- a. [obligation of states vs. corporate duty to respect]
- b. [HR are relevant for companies as per Ruggie Principles, especially with regard to online FoE, data protection, privacy]
- c. [Intermediaries as guardians of (and threats to) freedom of expression et al: functional consequences]
- d. [challenges of FoE in light of the four-dimensional matrix (state-user; state-intermediary; intermediary-user; user-user)]

- e. [taking up recommendations from Corporate Accountability Index 2015 (Ranking Digital Rights)]

3. [Selected human rights case studies]

- a. [Freedom of expression]
 - i) [Convention and Strasbourg – protection of FoE online]
 - ii) [Challenges of FoE in ‘private spaces’: will there be semi-public / public spheres online?]
 - iii) [Can public law override terms of service?]
 - iv) [Difference between expressions to be criminally punished under international law (advocacy of terrorism, advocacy of genocide, child abuse images, qualified hate speech) and different national legislations]
 - v) [legitimate content restrictions: blocking, filtering and takedown]
- b. [Data protection]
 - i) [economic dimension of user data: commodification of data]
 - ii) [protection of user data in light of national, European and international HR law; relationship to privacy; standards contained in Convention 108, especially 5.2.: free, specific, informed, unambiguous consent ... of the data subject ... or other legitimate basis laid down by law ...]
 - iii) [importance of transparency of data processing by intermediaries, especially regarding processes to give information about users to third parties (law enforcement, private parties) (quoting Convention 108: Article 7bis: “e) controller must provide the means of exercising the rights ... as well as an necessary additional information I order to ensure fair processing of the data”; Article 8 – automated data processing ... right to obtain knowledge of the reasoning underlying data processing ... (limited by e.g. trade secrets)]
 - iv) [use of “Necessary and Proportionate principles?]
- c. [Right to encryption/anonymity]
 - i) [Challenge regarding monetarization/commodification of data]
 - ii) [national decisions do not uphold right to be active online in private spaces]
 - iii) [human rights relevance especially in autocratic regimes]
 - iv) [right to be active ‘alone’ online?]
- d. [Right to be de-indexed]
 - i) [important example of ‘new’ right that was created by courts and self-administered/implemented by search engines]
 - ii) [success story? But Google ‘never wanted this role; over-extension of judicial authority; underframing of normative challenges; normative reaction by states or through judicial dialogue]
 - iii) [public interest test? role of states? judicial redress?]
- e. [Privacy]
 - i) [Link between privacy and data protection and right to privacy as a precondition for creating the safe space in which to exercise online rights]
 - ii) [Importance of clarity of privacy policies of Internet intermediaries]
 - iii) [Threat to privacy through pervasive online surveillance]
 - iv) [privacy by design as good practice]
- f. [Human rights aspects of big data and algorithms]
 - i) [ethical use of big data analytics by intermediaries]
 - ii) [preventive policies and risk assessment through intermediaries – legitimacy?]
 - iii) [empowerment of the human factor in big data supported decisions]

4. [Intermediary liability regime]

- a. [recent ECtHR jurisprudence leaves questions open]
- b. [problems with the often-used notice-and-take-down approach without independent judicial review (La Rue report 2013): design of procedure; general interest test]
- c. [issues with automated take-down systems]
- d. [minimum standards for any liability regime: [use of Manila Principles (MPII)² / differentiation]
 - i) Principle I, MPII: Intermediaries should be shielded by law from liability for third party content (especially d) intermediaries must never be made strictly liable for hosting unlawful third-party content, nor should they ever be required to monitor content proactively as part of an intermediary liability regime
 - ii) Principle II, MPII: Content must not be required to be restricted without an order by a judicial authority
 - iii) Principle III: Requests for restrictions of content must be clear, be unambiguous, and follow due process
 - iv) Principles IV, V: Laws and content restriction orders and practices must comply with the tests of necessity and proportionality and due process
 - v) Principle VI: Transparency and accountability must be built into laws and content restriction policies and practices

5. [Procedural guarantees]

- a. [due process must be ensured for all users regarding decisions impact their rights]
- b. [development of international due process standards through international intermediary and judicial dialogue]
- c. [relationship of internal monitoring to counter-speech approaches]
- c. [minimum requirements for transparent and accountable internal processes]
 - i) [transparency and accountability;
 - ii) availability of mechanisms to report illegal content;
 - iii) 'rule of law' equivalent/internal ADR processes
 - iv) process for third party claims;
 - v) notification of restrictions;
 - vi) judicial remedies]

6. [Overcoming conflicts of laws and jurisdictions]

- a. [territoriality as traditional anchor of law, but use of intermediaries challenges territoriality (cloud services): extraterritorialization of laws (legitimacy?) and forced reterritorialization]

² See Manila Principles on Intermediary Liability, Background Paper:
https://www.eff.org/files/2015/07/08/manila_principles_background_paper.pdf

- b. [applicability of laws to intermediaries dependent on incorporation? Service? Data location?]
- c. [Importance of state assessing impact of laws to avoid extraterritorial impact and, in particular, negative impacts on the transboundary flow of information]
- d. [development of transnational dialogue to solve issues of conflict of laws and jurisdiction: end to forum shopping, highest standard of human rights protection must prevail]
- e. [applied to jurisdiction]
- f. [applied to legal system applicable]
- g. [applied to effective enforcement through judicial cooperation]

7. [Criminal law]

- a. [future of application of criminal law on Internet intermediaries in a cross-border context]
- b. [difference between internationally criminalized speech and national standards – how to choose: clear ‘red lines’: terrorism, child exploitation, genocide, qualified hate speech]
- c. [access by criminal justice authorities to data in the cloud]
- d. [forensic access to intermediary data joint requests, emergency procedures]
- e. [solution: direct transborder cooperation – challenge of flexibilizing criminal procedure law and the law of evidence]

8. [Self-regulation]

- a. [importance of establishing self-regulatory frameworks regarding content moderation/search algorithms regarding all norms that influence the selection, aggregation and presentation of information by intermediaries (internal Intermediary norms, IINs)]
- b. [bottom-up development of IINs]
- c. [dangers of unchecked IINs, e.g.: commercial content moderation, through intermediaries]
- d. [importance of ensuring substantive and procedural transparency regarding development of IINs and challenges to IINs constitutionalization of IINs?]
- e. [recourse to courts and transnational due process framework regarding challenges to IINs]

9. [Accountability of governments when interfering in the normative ecosystem of Intermediaries]

- a. [protection of intermediaries from government interference by HR law; intermediaries as agents of the HR protection of their users]
- b. [maximizing human rights protection; minimizing human rights interferences – as the goal to any normative intervention into Internet intermediaries]
- c. [hard law - ECtHR, soft standards]
- d. [how to frame obligation to make governmental requests plainly visible in disaggregated form]
- e. [to that end: establishment of independent and effective judicial, administrative and/or parliamentary oversight mechanisms for the law and practice of Intermediaries with regard to and State intervention into, and use of, intermediaries, especially in relation to surveillance through intermediaries and data protection]

10. [Clarifying user rights vis-à-vis Internet intermediaries]

- a. [increasing 'normative literacy', providing readable terms of service]
- b. [attractivizing HR-sensitive freedom of expression 'management' frameworks]
- c. [importance of an enabling environment for both intermediaries and users]

11. [Development of accessible best practice repositories]

- a. [identification of existing best practice/best practice repositories]
 - i) [related to procedures]
 - ii) [related to content]
- b. [development of overarching transnational due process frameworks based on transnational multistakeholder dialogue]

Reference instruments

(list of relevant Council of Europe instruments)