CONFERENCE ON INTERNET FREEDOM
"THE ROLE AND RESPONSIBILITIES OF INTERNET INTERMEDIARIES"

Conference co-organised by the Austrian Chairmanship of the **OSCE** and the
Czech Chairmanship of the **Council of Europe** Committee of Ministers
13 October, 2017 | Hofburg, Vienna

Following the second joint Conference on Internet Freedom, held in Vienna on 13 October 2017, the organisers[1] of this event present a short summary of the **key conclusions and recommendations** and a comprehensive **conference report**, including detailed recommendations, prepared by the conference rapporteur[2].

KEY CONCLUSIONS AND RECOMMENDATIONS

− Internet intermediaries play an essential role in the digital ecosystem as gateways to information and facilitators of the exercise of the right to freedom of expression, freedom of assembly and association, education, access to information, knowledge and culture, participation in public and political debate and in democratic governance.

− States need to ensure that the internet remains an open network for the free flow of information and ideas, regardless of frontiers, and that any proposals to regulate the internet respect human rights and fundamental freedoms, online just as offline, including the right to freedom of expression.

− Given that the needs of society in the digital age are shifting and the role of internet intermediaries is constantly being expanded, all actors (states, private sector, civil society) need to urgently consider the scope of the intermediaries' duties and responsibilities and how they can be reflected in laws that both protect citizens and enable a dynamic internet environment.

− Companies and states should strive towards greater transparency, including in relation to the kind of content that is removed, the criteria that are applied, and the procedures in place in order to challenge over-removals. Similarly, due process safeguards must be put in place when intermediaries remove content, including through requirements to substantiate notices, the introduction of counter-notices and effective complaint mechanisms.

---

[1] This conference was co-organized by the Austrian OSCE Chairmanship and the Czech Chairmanship of the Council of Europe (CoE) Committee of Ministers, in partnership with the Austrian Federal Chancellery, the CoE Information Society and Action against Crime Directorate, and the Office of the OSCE Representative on Freedom of the Media.

[2] Conference Rapporteur: Matthias C. Kettemann (Cluster of Excellence "The Formation of Normative Orders", University of Frankfurt am Main (Germany) and Institute of International Law and International Relations, University of Graz (Austria).

Rapporteur: Matthias C. Kettemann (Frankfurt am Main/Graz)*****

1. Introduction

In 2017, the debate on the meaning of the notion of `Internet Freedom`, its limits and the challenges of its realisation continues unabated. The year after the first Internet Freedom Conference, organised jointly by the Council of Europe and the OSCE, on 9 September 2016 in Strasbourg (dedicated to Internet Freedom "as a Constant Factor for Democratic Change in Europe"), saw growing dissatisfaction among internet users, companies and states regarding the parameters of online communication.

Standards of both organisations confirm that states are responsible for keeping the internet an open and public space where freedom of expression can be effectively exercised and the same rights that apply offline also apply online. States therefore need to ensure an enabling environment for the exercise of human rights online. Given the structures and conditions of online communication today however, many of the decisions that impact the effective exercise of freedom of expression and other rights online are in fact taken by private companies.

These internet intermediaries play an essential role in the internet ecosystem: as gateways to information, facilitators of communication, and providers of a vast array of online services. Since users rely on them, standards applicable to intermediaries directly influence how freedom on the internet can be exercised. To avoid self-censorship motivated by sanctions, internet intermediaries are, as a general rule, shielded from liability for third party content as long as they expeditiously remove or disable access to this content once in knowledge of its illegality. But these conditions are in flux and the growing misuse of the internet as a medium to transmit hateful messages has put into question the parameters of these liability exceptions.

As a consequence, intermediaries have taken on a more active role in regulating online content and assessing its legality – sometimes by themselves, sometimes under pressure from states. Proactive monitoring, however, is deeply problematic in terms of human rights. Technological means to stop, for instance, the spread of "false" information, are imperfect. Blocking often leads to overblocking. Filters tend to be imperfect and regularly filter out perfectly legal content. Algorithms might be getting 'smarter', but are often not smart enough (programmed smartly enough) to respect human rights and avoid indirect discrimination. Importantly, at their current state, they are not able to assess context properly, and therefore not able to respond effectively without human intervention.

As the Council of Europe draft recommendation on the roles and responsibilities of internet intermediaries and the OSCE Representative on Freedom of the Media's various recommendations on Internet Freedom and Open Journalism demonstrate, states are confronted with the complex challenge of regulating an environment in which private actors perform crucial functions with significant public service value.

In light of the growing threats to human rights online, states have pressured intermediaries to act more decisively against illegal content and activities, including hate speech, child sexual abuse, incitement to violent extremism, radicalization and terrorism promotion. In short, private sector companies (particularly internet intermediaries) are asked to exercise more substantial control over internet content.

Recognising the need to do more with regard to developing policy in the area of freedom of expression on the internet, and deepening the OSCE participating in and Council of Europe member states' understanding and engagement on the questions surrounding roles and responsibilities of internet intermediaries, the Austrian Chairmanship of the Organization for Security and Co-operation in Europe (OSCE) and the Czech Chairmanship of the Council of Europe Committee of Ministers jointly organised the Second Internet Freedom Conference, on the role and responsibilities of internet intermediaries, on 13 October 2017 in Vienna, in partnership with the Austrian Federal Chancellery, the Council of Europe Information Society and Action against Crime Directorate, and the Office of the OSCE Representative on Freedom of the Media.[3]

2. Open questions

The report on the 2016 conference warned that „[i]f states do not provide the norms necessary to ensure internet freedom, private sector actors will (often reluctantly) fill the void with norms that may not be primarily in the public interest." It is the character and content of these norms, the roles and responsibilities of intermediaries, and the norms states should pass in order to ensure human rights protection online that the 2017 conference focused on.

Intermediaries help us communicate, search and pay online – and hence structure our online experience. They include a wide, diverse and rapidly evolving range of actors, facilitating interactions between natural and legal persons by offering and performing a variety of functions and services. Intermediaries may carry out several functions in parallel, but intermediary services may also be offered by traditional media companies. Any analysis must therefore focus on the function performed and not so much on the company performing it. It is this 'functional' approach that is a key normative element of all OSCE and CoE documents pertaining to internet freedom, including the CoE draft Recommendation on roles and responsibilities of internet intermediaries.

Taking into account the normative commitments and standards of the CoE and the OSCE, and recognising the dual focus of the conference on states and intermediaries, the four sessions of this conference tackled four interrelated questions:

---

[3] See, for the conference page, the websites of the Council of Europe and the OSCE, respectively. Video recording of the proceedings, concept paper and programme are all available online on the conference page (Council of Europe; OSCE).

- what is the current state of internet freedom across participating states of the OSCE and the CoE member states in terms of performance of states, performance of internet intermediaries and cooperation between them;

- what role social media and search engines have in shaping the public sphere and filling their role within;

- how intermediaries determine the unlawful nature of third-party content and which law and policy questions these processes raise; and

- how to develop an adequate legal and policy framework for securing internet freedom, including through a confirmation of liability exemptions and adjustment to content moderation through transparent procedures based on the rule of law.

3. Roles and responsibilities of states and intermediaries

3.1. Today's regulatory choices matter

Clemens Koja (Chairperson of the Permanent Council, Austrian OSCE Chairmanship) opened the conference by confirming that "[t]he regulatory choices that are made today will have a profound impact on the future of internet freedom" and that it is important to develop joint efforts. Roland Faber (Deputy Director General, Federal Chancellery of Austria) highlighted the importance of intermediaries as gateways to the facilitation of the exercise of freedom of expression and reminded participants of the importance of taking into account developments on the EU level as well. Harlem Désir (OSCE Representative on Freedom of the Media) reminded participants that "Facebook [reportedly] deletes 66,000 posts per week [including] journalists' articles", sometimes "upon the request of national governments. This leads to the question how safe media freedom is in the hands of private intermediaries."

Richard Kadlcak (Special Envoy for Cyberspace, Ministry of Foreign Affairs, Czech Republic), pointed to the standards developed by the Council of Europe that relate to intermediaries, and the draft Recommendation on the roles and responsibilities of internet intermediaries. Jan Kleijssen (Director, Information Society and Action against Crime Directorate, Council of Europe), reminded participants that fighting against illegal content necessitated close cooperation between "all actors, public or private", underscoring that "certain functions [...] are the ultimate prerogative of states, but internet companies do have a role to play based on clear, foreseeable and proportionate rules that fully comply with human rights, the rule of law and democratic values. Importantly, these companies should not replace parliaments or courts.

3.2. Session I: Taking stock of internet freedom[4]

---

[4] Thomas Schneider (Ambassador and Director of International Affairs, Swiss Federal Office of Communication (OFCOM), Federal Department of the Environment, Transport, Energy and Communications (DETEC)) as moderator; Yaman Akdeniz (Professor, Istanbul Bilgi University), Walter Berka (Professor, University of Salzburg), Karmen Turk (Media law attorney, Tallinn, Estonia), Xianhong Hu (Division for Freedom of Expression and Media Development, UNESCO).

Session I focused on the current state of internet freedom in terms of states' performance regarding internet freedom, on how states and intermediaries cooperate and how intermediaries, through their standards, contribute to ensuring rights online.

Taking stock of the state of internet freedom across the OSCE and Council of Europe states, speakers pointed out that despite the existing human rights framework with its standards and instruments, a number of states in the Council of Europe/OSCE region applied laws in a way that resulted in blocking of content and takedown of websites, which was not proportionate to the legitimate aims pursued.

Speakers also highlighted the importance of internet freedom as a holistic approach that influenced states' activities, especially with regard to the "internal balance" of internet-related policies, such as those related to cyber-security, privacy protection, content moderation, etc. This balance also had to be struck between the positive and negative obligations of states and the obligations of private actors.

The panel identified the lack of clear rules with regard to the responsibilities of private actors as a factor of uncertainty, especially those exercising intermediary functions. In the absence of clear rules, governments can exercise pressure on internet intermediaries to delete legal content by threatening sanctions or asking for informal cooperation. This instigates proactive self-censorship by intermediaries and overblocking of legal content. The speakers also encouraged a graduated and differentiated approach, taking into account the different functions in all regulative approaches to intermediaries. Intermediaries were also criticized for operating key aspects of their business, especially central operational algorithms, inside a 'black box'. While understandable for business reasons, this lack of transparency is problematic for governments wishing to introduce legislation targeting algorithmic discrimination, and for the wider public in understanding the way how information they seek, receive, and impart is shaped. As a first normative step, the EU General Data Protection Regulation contains a limited right to explanation regarding the logic behind algorithms used by data controllers, which most intermediaries are.

The speakers encouraged the use of existing normative instruments, including the Council of Europe Committee of Ministers Recommendation on Internet Freedom (2016/5) and Recommendation on a New Notion of Media (2011/7) which had established the concept of a graduated and differentiated approach. The panel also strongly encouraged the use and sharing of national case studies in order to successfully implement the Recommendation on Internet Freedom and ensure that 'lessons learned' on increasing internet freedom were shared across Europe.

3.3. Session II: Social media and search engines as global scale editors[5]

Session II focused on the role that social media and search engines – as *de facto* global scale editors – have in shaping the public sphere and in filling their role within, especially in light of

---

[5] Tarlach McGonagle (Institute for Information Law, University of Amsterdam) as moderator; Marco Pancini (Director of Public Policy and Government Affairs, Google); Elena Sherstoboeva (Associate Professor of the Higher School of Economics, Moscow); Ingrid Brodnig (Digital Ambassador of Austria to the EU); Maximillian Schubert (EUROISPA).

the associated challenges from the perspective of a free and informed debate, the free flow of information and democratic values.

Speakers agreed that "fake news" has always existed. However, the realities of online communication and psychological factors regarding the uncritical consumption of internet-based content have made the phenomenon much worse.[6] A number of studies have shown that even if internet intermediaries, neither wanted to nor had actually become global editors, they still substantially impacted how people saw the world and how they acted.

The panel referenced the *Tamiz v. UK* inadmissibility decision (para. 84),[7] in which the Court citied normative approaches by the Council of Europe, the EU, the UN and the OSCE as having "indicated that [intermediaries] should not be held responsible for content emanating from third parties unless they failed to act expeditiously in removing or disabling access to it once they became aware of its illegality". Speakers agreed that this principle should apply to all intermediaries. Nevertheless the speed, scale and complexity of the means through which intermediaries implemented removal might vary by the size and commercial nature of the intermediary.[8] Similarly, the draft Recommendation takes the approach that the higher the impact and the potential damage to the objects of legal protection and the higher the value of the services for the exercise of human rights, the greater the precautions must be that the intermediary must employ when ensuring the removal of illegal content. The distinction between host/content provider and the relevant exemptions in the EU E-Commerce Directive still had some relevance, but the ecosystem and multi-functionality of intermediaries made things much more complicated.

Intermediaries have evolved into complex multifunctional organisms with global responsibilities. Any regulation, the panel confirmed, needed to take a graduated and differentiated approach and should respect the principles of legal certainty and foreseeability. States should refrain from encouraging the privatisation of law enforcement but rather continue to uphold due process values and practices without further informal incentivisation to the removal/blocking/filtering of content.

The panel concluded that users needed to be more aware of their rights online. Speakers identified the need to mainstream media and digital literacy into school curricula and roll them out as part of 'life-long' learning strategies.

3.4. Session III: Determining the illegality of third-party content[9]

The third panel discussed the procedures and standards used by intermediaries to determine the unlawful nature of third-party content and the impact of algorithms on these processes.

---

[6] See Claire Wardle, Hossein Derakhshan, "Information Disorder: Toward an interdisciplinary framework for research and policy making", Council of Europe report DGI(2017)09.

[7] ECtHR, *Tamiz v. the United Kingdom* (dec.), application no. 3877/14, 19 September 2017.

[8] The European Court of Human Rights confirmed this approach in *Pihl v. Sweden* (dec.), application no. 74742/14, 7 February 2017.

[9] Ben Wagner (Assistant Professor, Vienna University of Economics and Business) as moderator; Aibhinn Kelleher (Associate Policy Manager, Facebook); Martin Husovec (Assistant Professor, University of Tilburg); Arzu Geybullayeva (freelance journalist); ~~Niels Lestrade (Project Manager, National Police Intelligence Unit, Netherlands);~~ Dan Shefet (attorney).

The panel pointed out that states had a tendency to delegate the task of determining what was unlawful to private parties. This was unfortunate because intermediaries as profit-maximizing entities did not have *prima facie* political accountability and were not mandated to perform the role of judges regarding the legality of content. They may also err on the side of caution to avoid government complaints, which consequently may lead to unnecessary and excessive censorship. However, as the example of the partly privatised responsibility in the fight against money-laundering (reporting obligations for banks) showed, some responsibilities may be legitimately privatised.

A panellist representing an internet intermediary expressed that they were very careful when removing content. Before users were identified as 'terrorists' (and their content deleted), their comments were carefully considered. These assessments could not be automated and therefore took time.

Speakers also argued that normative frictions arose between the exceptions from liability systems in the US and in Europe. Even if a company was liable under the E-Commerce Directive, it might enjoy (relative immunity) under US law. Diverging intermediary rules lead to legal uncertainty.

Panellists agreed that algorithms and automated systems could be used to support human decisions and scale them, but should not be able to take 'their own' decisions with regard to illegality of content. Whether or not content is merely objectionable or unlawful is a question deeply connected to the social fabric of society, something even trained judges were often having difficulty with. But with regard to specific identifiable content, automation could be very useful. Automatic tools could, for instance, disable the upload or re-upload of "revenge porn" or pictures connected to the exploitation of children.

3.5. Session IV: An adequate legal and policy framework for securing internet freedom[10]

This session presented views on the best legal and policy framework for securing internet freedom by providing best practices examples and normative red lines regarding two key issues, namely the confirmation of liability exemptions and adjustment to content moderation through transparent procedures based on the rule of law.

Speakers discussed the current EU approach based on identification, removal and avoidance of reappearance of illegal (rather than merely harmful) content. The current Communication[11] in the European Commission's assessment, provided good practices for the protection of due process and freedom of expression. It recommended that companies should ask for more substantiated notices, the trusted flagger system should be made more transparent and subject to certain conditions; transparency reporting, which allowed users to

---

[10] Gabrielle Guillemin (Article 19) as moderator; Joe McNamee (EDRi); Robert Spano (Judge, European Court of Human Rights); Daniel Holznagel (Federal German Ministry of Justice and Consumer Protection); Irene Roche-Laguna (DG Connect, European Commission).

[11] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Tackling Illegal Content Online Towards an enhanced responsibility of online platforms" (28 September 2017, COM(2017) 555)

know about content-related interactions between states and intermediaries, and the application of intermediaries' own content-related policies, should be standardised; systems of counter-notice should be put in place; the use of algorithms should involve at least some human intervention ('human in the loop' principle); and more cooperation should take place between the various stakeholders, including company representatives, civil society, engineers and academics, and policy-makers from international organisations and states.

The German Netzwerkdurchsetzungsgesetz[12] was presented as an example of national legislation to ensure that intermediaries police their platforms effectively. According to the government's view, the law did not require companies to do anything more than they were already required to do, i.e. comply with the law. The law had been enacted because companies had been too slow in removing illegal hate speech and content which was manifestly illegal. The law's scope was limited to certain provisions of the criminal code such as holocaust denial. Companies were only required to remove content within 24 hours when the content was manifestly illegal but otherwise had up to 7 days to deal with complex cases. The law introduced fines, but only for systemic failures to comply with the law. The law also required companies to be transparent about the procedures put in place and their effectiveness. Another important element was the establishment of a national contact point.

Speakers also underscored that any intermediary liability framework needed to be holistic. A distinction should be made between commercial and non-commercial actors as well as between active and passive intermediaries. In *Delfi*, the ECtHR had made clear that liability could be imposed on intermediaries when they failed to take measures "to remove clearly unlawful comments without delay, even without notice from the alleged victim or from third parties" (§ 159).[13] It was important to put in place graduated content responsibility and due process safeguards and ensuring that cases could be adjudicated independently.

The panel also discussed adequate responses to illegal content online. Any response needed to respect human rights, in particular the principle of legality, which applied both to states and EU institutions. So-called voluntary measures, promoted by the European Commission and some member states, entailed a lack of transparency and accountability, particularly in relation to removal of content. Encouraging voluntary measures allowed states to implement an approach that they were prohibited from imposing (such as a general obligation to monitor content).

3.6. Closing session

After preliminary conclusions by the rapporteur, Matthias C. Kettemann (University of Frankfurt/Main, University of Graz), two representatives of the conference organisers concluded the conference. Richard Kadlcak, Special Envoy for Cyber Space, Ministry of Foreign Affairs, Czech Republic, and Gerhard Doujak, Human Rights Director, Ministry of Foreign Affairs, Austria, lauded the conference's success in providing a platform for the sharing of experiences and best practices on one of the most pertinent challenges to media freedom in the digital age. Underlining the need for more transparency about content regulation and refusal to rely on technological solutionism, the conference organisers again highlighted the importance of the effective protection of freedom of expression, which lay at

---

[12] Netzwerkdurchsetzungsgesetz vom 1. September 2017 (BGBl. I S. 3352).
[13] ECtHR, *Delfi AS v. Estonia* (GC), application no. 64569/09, 16 June 2015.

the core of human activity online.

4. Recommendations

The second Internet Freedom Conference brought together key stakeholders who examined how internet intermediaries as gatekeepers to the exercise of freedom of expression online can be regulated in a human rights-sensitive way.

Grounded in the recommendations developed during the first OSCE/CoE joint Internet Freedom Conference in 2016, and further developed by interventions of speakers and discussants, the following recommendations regarding the role and responsibilities of internet intermediaries in the digital age can be formulated.

General recommendations

- Intermediaries play an essential role in the digital ecosystem as gateways to information and facilitators of the exercise of freedom of expression, freedom of assembly and association, the right to education, access to information, knowledge and culture, participation in public and political debate and in democratic governance. States have to engage with them in order to ensure that they, the states, can fulfill their obligation to ensure to anyone under their jurisdiction all applicable human rights and freedoms, online just as offline.

- Given that the needs of society in the digital age are shifting and the role of internet intermediaries is constantly being expanded, all actors (states, private sector, civil society) need to urgently consider the scope of the intermediaries' duties and responsibilities and how they can be reflected in laws that both protect citizens and enable a dynamic internet environment.

- Any regulation to be implemented must be read in light of the commitment of all Council of Europe member states and OSCE participating states, to the protection of fundamental human rights and freedoms (both online and offline), particularly the right to freedom of expression "regardless of frontiers", and the rule of law, and in line with the shared understanding of internet freedom rooted in international obligations and responsibilities of the respective participating and member states, particularly those drawn from the International Covenant on Civil and Political Rights, the European Convention on Human Rights and the OSCE commitments as well as other relevant standards.

- The concept of Internet Freedom should remain a holistic approach, which should not be balanced against other rights and freedoms. It is essential for states to learn from best practices, for instance by implementing the indicator-based Internet Freedom reporting model pioneered by the Council of Europe in its 2016 Recommendation without undue delay.

- A clearer understanding that today's regulatory choices have a profound impact on the future of internet freedom, the dynamism and economic potential of the digital environment, and the realisation of all human rights by all online need to be promoted among all stakeholders.

Recommendations for states

- In the definition and normative framing of the roles and responsibilities of intermediaries, states have a powerful role to play in the digital ecosystem, and shall exercise this role responsibly.

- States are obliged to respect the rule of law and support internet freedom both internally and internationally. Any new laws must thoroughly be assessed in light of their human rights impact. Any decisions by state authorities interfering with human rights must be based on law, pursue a legitimate aim and be proportionate to this aim. In particular, any state action must respect Article 19 of the ICCPR.

- In particular, states should further engage with the Office of the OSCE Representative on Freedom of the Media and with the Council of Europe, and implement the recommendations coming from these institutions. In doing so, they should cooperate actively with civil society in order to develop a complete picture of how internet freedom is progressing.

- Before passing new laws impacting the activity of intermediaries, states need to take into account international human rights standards and conduct human rights impact assessment. Similarly, states need to explore the practices of intermediaries, in cooperation with the latter where appropriate, before making public policy decisions.

- Social media companies and search engines, in particular, have substantial power in managing what content people see. Applying traditional media law to all of their functions cannot be effective in light of their special and often ambivalent role. Yet they exercise the role of global content managers, and international and national standards must ensure that the intermediaries' powers are exercised responsibly. The law must be tailored to the functions they exercise and normative approaches need to be graduated and differentiated.

- States cannot assign intermediaries the role of 'judges' regarding the legality of content, as decisions taken outside the rule of law frameworks risk leading to restrictions of freedom of expression that fall short of the requirements of legality, necessity in a democratic society, and proportionality with a view to a legitimate aim. They must provide clear guidance as to what action is illegal and what is not. Unclear cases where a balancing of rights has to be performed must be decided by a national authority that is competent to do so, which includes a clear judicial process and not by a private entity.

- Further, law enforcement cooperation with intermediaries needs to be refined as it often suffers from administrative, communicative and legal hurdles. States must ensure clarity of their legislative frameworks related to law enforcement and apply them with sufficient predictability, to enable intermediaries to cooperate effectively while fully respecting their responsibilities with regard to human rights and fundamental freedoms.

- States need to establish and support, in cooperation with intermediaries where appropriate, digital literacy and media literacy programmes in order to enable young people to use the internet as a tool of empowerment.

Recommendations for internet intermediaries

- Internet intermediaries play an essential role in enabling the exercise of human rights and fundamental freedoms online. Recognising that intermediaries have certain (if limited) negative and positive duties to respect human rights in their sphere of activity and with regard to all affected parties is an important step towards ensuring human rights online.

- Recognising the increasing pressure on internet intermediaries to further control online content, intermediaries need to expand their capabilities to balance human rights and fundamental freedoms of involved parties. In particular, intermediaries should act as transparently as possible. With their growing role comes greater responsibility. Just relying on algorithms cannot suffice - on the contrary, it can in fact be problematic. Intermediaries operate in a challenging legal ecosystem and should be treated according to the functions they exercise. States, for their part, should encourage intermediaries to shed light onto the black box of processes and practices employed for content management.

- Situations in which intermediaries implement national enforcement decisions and those where they voluntarily take down content have to be distinguished. However, in both cases, decisions should be taken only on the basis of predictable and transparent rules, based on due process or other applicable procedural guarantees, and any processes leading to interferences with the right to freedom of expression of users and other affected parties should be as open and transparent as possible.

- Penalties may incentivize over-compliance and over-blocking. Intermediaries should not be responsible for content of third parties unless they fail to act expeditiously to remove it upon being made aware of the content's illegality. Liability exceptions as a general rule for hosted content should thus not be touched. The existing model of notice-and-action should, however, be refined to meet the role intermediaries exercise today, by adding for instance minimum content requirements and standardised flagging processes, including the possibility for affected parties to challenge removals and clear avenues for organisations to become trusted flaggers.

- Transparency reporting should ideally be standardised in order to allow for more meaningful comparisons and ensuring compliance with any applicable legal framework.

- Companies and states should strive towards greater transparency, including in relation to the kind of content that is removed, the criteria that are applied, and the procedures in place in order to challenge over-removals. Similarly, due process safeguards must be put in place when intermediaries remove content, including through requirements to substantiate notices, the introduction of counter-notices and effective complaints mechanisms.

- A graduated approach to content liability seems to be the way forward, whether based on the activity of the provider at issue or the particular type of content involved. Any approach to liability should be based on the human rights framework and on lessons learnt from previous policy approaches.

- Algorithmic decision-making, machine-learning and semantic technologies are

increasingly utilised by companies to help cope with the huge number of removal decisions that need to be taken on a daily basis. With regard to specific illegal content, such as 'revenge porn', child sexual exploitation images and the promotion of terrorism, there is a need for prompt reaction to prevent the redistribution of such illegal content. Nevertheless, unintentional side-effects and indirect indiscrimination caused by algorithms should be countered by demanding more openness regarding the design and use of algorithmic decision-making. Advances in AI technology, including self-learning, , a human should be in the loop when decisions on legality of content are taken.