CONTENT REGULATION AND HUMAN RIGHTS IN THE DIGITAL AGE

Multi-Stakeholder Roundtable on the Digital Services Act

4 June 2020 — 4pm CEST / 10am EDT / 7am PDT

Roundtable Report

On June 4, 2020, the Global Network Initiative (GNI) hosted a multistakeholder roundtable discussion to examine key provisions of the European Union's anticipated Digital Services Act (DSA) through the lens of international human rights law and principles. This event followed a public discussion hosted by GNI that was held on May 28 and featured UN Special Rapporteur David Kaye and Council of Europe Commissioner for Human Rights Dunja Mijatović.

Participants were provided a draft of GNI's forthcoming policy brief, "Content Regulation and Human Rights in the Digital Age," which was presented as a framework for considering good policy practice. Though many human rights are impacted by content regulation, controls on communication most directly impact fundamental rights to freedom of expression and privacy. The policy brief and our discussion thus focused on these two rights.

Member of the European Parliament Alex Agius Saliba, who serves as the DSA Rapporteur in the Committee for Internal Market and Consumer Protection, delivered opening remarks. The subsequent discussion focused on four key components of the DSA, each introduced and moderated by a different GNI member: (i) scope of content and services; (ii) notice-and-action framework; (iii) transparency requirements; and (iv) enforcement and remedy.

As content regulation initiatives continue to be introduced and implemented around the world, GNI believes proactive and honest multi-stakeholder conversations on this topic are key to ensuring that responses to digital harms are legal, proportionate, and fit-for-purpose. GNI looks forward to further consultations on the DSA and other content regulation efforts.

The conversation was held under the Chatham House Rule. Nothing in this report is attributed to any individual, institution, or affiliation, nor does it necessarily reflect GNI's position.

Table of Contents

A Brief Introduction to the Digital Services Act

The Electronic Commerce Directive ("e-Commerce Directive") adopted by the European Union in 2000 established an internal market framework for the provision of online services across Member States. This framework sought to remove obstacles to cross-border e-commerce activity within the EU by creating a shared understanding among member states and harmonizing member state approaches. It included "safe harbors" for online intermediaries for user-generated content and prohibited member states from placing general monitoring obligations upon intermediaries.

The digital ecosystem has changed significantly in the 20 years since the e-Commerce Directive went into effect, and member states have responded to new challenges in varied ways, including by enacting content regulations at the national level. With the Digital Services Act (DSA), policy makers seek to update the e-Commerce Directive by addressing these new challenges and again harmonizing Member State approaches. The DSA will shape the digital economy of the European Union but also will likely impact corporate compliance globally and provide a model for content regulation to the rest of the world, as the EU General Data Protection Regulation did for data protection.

Rapporteurs of three parliamentary committees — Internal Market and Consumer Protection (IMCO), Civil Liberties (LIBE), and Legal Affairs (JURI) — have issued preliminary reports with recommendations for the shape and content of the DSA.

A Human Rights-Based Approach to Content Regulation

The roundtable began with an overview of the analytical framework used in GNI's forthcoming policy brief, "Content Regulation and Human Rights in the Digital Age."

The brief was developed in response to an increase in governmental efforts around the world that claim to address various forms of harm related to user-generated online content, which we refer to as "content regulation." It uses a human-rights based approach to analyze content regulation measures from a dozen countries around the world.

International human rights law reminds us to put individual rights at the center of efforts to improve our shared digital spaces. This is critical because these spaces and services remain primarily devoted to acts of communication. History has repeatedly shown the perils of efforts to govern communication that put majoritarian interests above the rights of individuals, journalists, critics, and dissidents.

The brief demonstrates that the norms and principles articulated in international human rights law provide a universal, time-tested, and robust framework that can help lawmakers find creative and appropriate ways to engage stakeholders, reconcile different interests, and mitigate unintended consequences of content regulation.

The brief examines content regulation efforts for their compatibility with three key principles of international human rights law: legality, legitimacy, and necessity. It also considers proportionality as a component of necessity and extends this analysis to privacy.

Legality

The principle of legality establishes that restrictions on freedom of expression must clearly define that which is prohibited and that which is allowed, "to enable an individual to regulate his or her conduct accordingly."[1] Such laws must also enable those responsible for their execution to ascertain expression that is allowed and that which is not, which contributes to predictable, consistent, and non-discriminatory enforcement. This is particularly important when laws rely on private bodies, rather than democratically-accountable regulators or independent judiciaries, to adjudicate and enforce such restrictions.

[1] UN Human Rights Committee, General Comment No. 34: Article 19 (Freedoms of opinion and expression), 102nd Sess, adopted 12 September 2011, UN Doc CCPR/C/GC/34, online: < https://undocs.org/CCPR/C/GC/34>.

Ambiguous content regulations can have a "chilling effect" on legitimate speech. In practice, chilling effects unfold in two ways. First, individuals who fear violating the law may shape their communications to avoid any potential implication, sometimes choosing not to speak at all. Second, intermediaries held liable for user-generated content may be overly broad in their enforcement of the law to prevent any possible infringement.

Legitimacy

The principle of legitimacy holds that laws restricting expression can only be justified to achieve specific, enumerated purposes. These may include respect for the rights or reputations of others or the protection of national security, public order, public health or morals. While international law gives states significant latitude to determine the activities that justify restrictions, that discretion is not unlimited. International courts and authorities have made clear that the right to freedom of expression is broad and encompasses "even expression that may be regarded as deeply offensive."

In addition, numerous consensus United Nations resolutions establish that offline rights must also be protected online. Inconsistencies in the treatment of online and offline speech may be exploited by regimes and actors who do not respect democratic norms. Therefore, it is critical to protect speech equally and consistently, and to resist differentiating approaches to expression across offline and online mediums.

Necessity and Proportionality

The principle of necessity requires states seeking to restrict expression to articulate the threat imposed by a specific type or piece of speech as well as the "direct and immediate" connection between the expression and the threat.

The related principle of proportionality requires that any restrictive law, as well as the actions of administrative and judicial authorities in their application of that law, must be: (i) proportionate to the interest being protected; (ii) appropriate to achieve that protective function; and (iii) the least intrusive instrument among those which might achieve that protective function.

In the content regulation context, the principles of necessity and proportionality should guide lawmakers to think carefully about which types of services are most appropriately positioned to address specific concerns. Shifting liability for illegal content from creators to intermediaries rarely if ever fits this description. Similarly, punitive sanctions, rigid timelines for content

adjudication, and pre-emptive filtering requirements are also likely to run afoul of the necessity and proportionality principles, and as such are likely to prove ineffective or counterproductive.

To ensure content regulation efforts are appropriately and narrowly tailored and to guard against unintended consequences, lawmakers should look to proven approaches based on concepts like transparency, due process, and remedy. They should also consider the perspectives of and, where appropriate, provide explicit protections for specific actors such as journalists and vulnerable groups.

Privacy

Many content regulation efforts lack protections for the fundamental right to privacy at best and, at worst, actively undermine individual privacy. Requirements to proactively monitor, track, or trace content often lack consideration of associated privacy risks. In addition, compelling content hosts to proactively report user-generated content and associated data to law enforcement agencies further undermines this right. Moreover, the explicit prohibition or implicit limitation of the use of anonymity and encryption tools signals a disregard for the importance of privacy and the rights it enables.

Scope

***Agenda Prompt**: The DSA will need to define what companies and/or services will be subject to its rules and enforcement, as well as the types of content and behavior. What are the pros and cons of different approaches to scope of services and content?*

The principle of legality requires that these components be precisely defined and clear to those required to observe and enforce the law. In addition, policy makers should carefully consider who should decide who sets the rules of what is in scope or not, with safeguards for human rights built into any outcomes.

Where laws do not meet this standard, ambiguity can result in unintended consequences that raise human rights concerns. Ambiguous content regulations can have a "chilling effect" on legitimate speech, as individuals may shape their communications to avoid any potential violation of the law, and - even more significantly - intermediaries which may be held liable for user-generated content will be strongly incentivised to take an overly broad approach in their enforcement of policies restricting certain forms of content to prevent possible legal penalties.

Scope of companies and services

The digital ecosystem comprises a wide range of ICT companies of different sizes, each with their own features and user base. The DSA will steer regulation of large social media companies, but it is unclear whether this guidance will also impact companies with other functions – such as web hosts, DNS providers, email providers, and more. While the reports focus largely on platforms that facilitate the generation and sharing of content and other forms of communications, further clarity on this point is needed. The principles of necessity and proportionality should guide lawmakers to think carefully about which types of services are most appropriately positioned to address specific concerns, and, where concerns exist, whether there is a need for different rules or obligations for different types of companies.

Scope of content and behavior

The rapporteurs' reports each take a different approach to the scope of content that should be covered in the DSA. The DSA should seek to define terms in ways that would avoid creating conflict with the international and domestic human rights obligations of member states. Looking at other jurisdictions that have introduced or enacted content regulations, many seek to regulate both illegal content and content that, though legal, may also be harmful. Some

content that would be considered harmful but not illegal may be protected expression. Even where definitions are clear and precise, requiring companies to make determinations about the legality of content may negatively impact democratic checks and balances, due process, and principles of oversight and accountability.

It is also important to consider the perspectives of and, where appropriate, provide explicit protections for specific actors such as journalists and vulnerable groups, which helps ensure content restrictions are truly necessary and proportionate.

An open question is how other EU efforts will influence and be influenced by the DSA. The 2016 Audiovisual Media Services (AVMS) Directive guides audio and visual content; it does not include non-audio or non-visual content. The Copyright Directive also will shape company action. In addition, the draft Terrorist Content Online Regulation includes a broad definition for terrorist content. The EU has also developed voluntary codes of conduct on hate speech and disinformation, which are already generating certain compliance-related results and may evolve into something more binding.

Notice and Action Framework

***Agenda Prompt**: How can the DSA help harmonize a rights-respecting approach to notice and action? Who should be able to trigger notice? What information should notices contain? How can the DSA anticipate and address misuse or abuse of such a framework?*

Human rights safeguards in notice and action systems have been the subject of robust discussion over the past 15 to 20 years. As a result, there is a significant body of existing resources on notice and takedown procedural protections that should be referenced as deliberations on the DSA framework continues.

More effort should be spent understanding novel challenges and how to overcome them. Rigid timelines around content removal and pre-emptive filtering requirements will pose threats to user privacy and incentivize over-removing content, drawing into question the proportionality of these approaches. Some governments have proposed a "duty of care" for intermediaries; the interaction of "duty of care" with a notice and action system should be carefully considered.

Notice mechanisms for illegal content should be distinguished from those for non-illegal content. Depending on whether content is illegal or non-illegal, and for illegal content whether the infraction is civil or criminal, a notice and notice framework should also be considered. Further, consideration of the process by which content is delivered to users may produce more useful and fit-for-purpose interventions to respond to non-illegal content.

Legally valid notices should include reference to the specific piece of content in question, as well as the specific legal authority under which the notice is being served. In addition, a counter notice, or the ability to challenge a claim to illegality, helps ensure due process. Including penalties for notices sent in bad faith will help reduce abuse of the system by bad actors.

Questions that emerged during discussion included:

- What kinds of content would be subject to a notice-and-action system? If non-illegal content is included, this raises further questions regarding enforcement and remedy (see **Enforcement & Remedy** section in this report).
- What is the relationship between safe harbor for content and larger systems of content regulation?
- What is a duty of care, and how does that impact a notice-and-action system?

Transparency Requirements

***Agenda Prompt**: Among other related topics, we will discuss what should be included in company transparency reports, considerations for algorithmic auditing, and the crucial complementarity of both corporate and government transparency.*

Each rapporteur emphasized the need for greater transparency and accountability around content moderation, digital advertising, and the use of algorithms. The reports also each envisaged an independent body that would oversee the implementation of transparency commitments and obligations. The availability of data will help facilitate independent oversight of both companies and government.

To ensure content regulation efforts are appropriately and narrowly tailored, and to guard against unintended consequences in their implementation, lawmakers should look to proven approaches to transparency, considering both company and government responsibilities.

Corporate Transparency

Over the last few years, large platforms have consistently reported on the number and, more recently, types of government requests for user data they receive. Some have also begun reporting on how they enforce their own content policies across various products, as well as the action taken as a result of that enforcement. However, few companies report data on their use of automated tools and associated outcomes. The patchwork of reporting mechanisms used by different companies is in part a result of their different service offerings and business models. At the same time, the varied approaches makes it challenging to compare those functions that are similar.

There is greater need for transparency around the use and impact of algorithms for curation, moderation, and recommendation of user-generated content and advertisements. A robust transparency mechanism could increase understanding of issues and harms, in turn contributing to more precise interventions that help protect expression and other rights.

Some companies publish public libraries of advertisements deployed through their products. Though a good step toward more transparent practices, more granular data, such as data related to engagement and delivery, is needed. Companies could also provide greater clarity and transparency around the policies guiding advertising content and targeting. It is important to consider the role that independent academics and other stakeholders can play in providing objective analysis and oversight, and not focus exclusively on information sharing with

governments. The IMCO and JURI rapporteurs both refer to "algorithmic auditing," which is proposed as a practice in which an independent auditor surveys an algorithmic system for the potentially harmful outcomes it may cause. The reports could provide more detail on what this would entail or how it would be conducted.

There is growing support for mandatory corporate due diligence. Earlier this year, European Commissioner for Justice Didier Reynders committed to developing legislation to make human rights due diligence mandatory for EU companies, which will likely include minimum requirements on transparency and reporting.

Government Transparency

The DSA should apply transparency and accountability requirements to governments as well. This includes both enabling companies to publish content removal orders they receive, where appropriate, as well as requiring government publication of information about orders sent, including the order's legal basis, whether it is for a civil or criminal offense, and details on the requesting government agency. For example, as the EU and member states increasingly use Internet Referral Units to address content – effectively shifting adjudication to companies' terms of services rather than domestic law – ensuring the transparency of these efforts and their outcomes will be an essential safeguard. Parliament's language in an earlier draft of the proposed EU Terrorism Content Online Regulation reflected positive transparency requirements for governments, but in the most recently leaked draft these requirements appear to have been substantially weakened.

Enforcement & Remedy

***Agenda Prompt**: Will the DSA modify current liability rules under the E-Commerce Directive and member state law? How will any new centralized enforcement authority interact with and impact member state enforcement authorities? What role can independent dispute resolution mechanisms play in facilitating user redress? How will the DSA impact existing platform efforts to facilitate appeals of content moderation decisions?*

Each rapporteur calls for the establishment of a central regulatory authority, and recommends continuing the e-Commerce Directive's prohibition against general monitoring obligations. Two reports also call for the establishment of dispute settlement mechanisms.

It is important to recognize the distinction between remedy for illegal content, which can include government enforcement of criminal laws, and the empowerment of users to seek appropriate redress for content that is not illegal but may be/have been restricted pursuant to companies' terms of service. In addition, there are other ways to empower users, including improving the "portability" of a user's data so that it can be moved from one platform to another. In sum, appropriate remedies will differ depending on context.

The international law norms of proportionality and comity should be of central consideration to the design and enforcement of the DSA. Achieving the right balance of prescriptiveness and flexibility will help ensure respect for fundamental rights and a healthy ecosystem amid a changing digital landscape. This would include, for example, recognizing that there is a spectrum of responses that platforms can apply to potentially infringing content, including but not limited to removal. Shifting liability for illegal content from creators to intermediaries rarely - if ever - fits these principles, particularly when combined with significant penalties for noncompliance. Enforcement focused on elements of due process, transparency, and remedy offer time-tested mechanisms to help ensure regulations are appropriately and narrowly tailored and help guard against unintended consequences.

Finally, it will also be important to ensure that procedures for accountability and dispute resolution are tailored in ways that account for the problem of scale and also preserve innovation and flexibility. On the one hand, simply shifting liability to companies is likely to lead to disproportionate responses. On the other, specifying a particular procedure and remedy for every dispute over content would be impossible to apply at scale and could also be subject to abuse. Moreover, a regulation that is too fixed in its approach would not be able to evolve to take account of changes in technology. An approach that sets broad expectations regarding due process and remedy and requires platforms to demonstrate the steps they are taking to resolve

disputes would be better suited to leveraging the knowledge and expertise of platforms in innovating to respond to these challenges.

In finding this balance, it may be useful to draw insights from an emerging movement in the context of business and human rights aimed at requiring companies to engage in due diligence to identify, mitigate, and remedy human rights harms that they are responsible for or with which they are linked. Regulators will also need to consider any overlap between requirements in the context of digital rights and these new due diligence laws, such as the 2017 law of vigilance in France.

About the Global Network Initiative

The Global Network Initiative (GNI) was launched in 2008. Our mission is to protect and advance freedom of expression and privacy rights in the information and communications technology (ICT) sector by setting a global standard for responsible decision making and serving as a multistakeholder voice in the face of government restrictions and demands. GNI members include ICT companies, civil society organizations (including human rights and press freedom groups), academics, academic institutions, and investors from around the world.

For more information, please visit our website: www.globalnetworkinitiative.org.

Appendix 1: Recommended Reading

Security Experts' Letter on Transparency in Terrorist Content Moderation (15 June 2020)

Tackling targeted ads and algorithms: RDR releases methodology for 2020 (Ranking Digital Rights, 8 June 2020)

Broad Consequences of a Systemic Duty of Care for Platforms (Daphne Keller, 1 June 2020)

Systemic Duties of Care and Intermediary Liability (Daphne Keller, 28 May 2020)

Human Rights: Our Best Toolbox for Platform Accountability (Ranking Digital Rights, 27 May 2020)

Commissioner Reynders announces EU corporate due diligence legislation (European Coalition for Corporate Justice, 30 April 2020)

Transparency Requirements for Digital Social Media Platforms: Recommendations for Policy Makers and Industry (Transatlantic Working Group on Content Moderation Online and Freedom of Expression, February 2020)

Facebook and Google: This is What an Effective Ad Archive API Looks Like (Mozilla, 27 March 2019)

Understanding the Human Rights Risks Associated with Internet Referral Units (Jason Pielemeier & Christopher Sheehy, 25 February 2019)

The Transparency Reporting Toolkit: Content Takedown Reporting (Spandana Singh & Kevin Bankston, 25 October 2018)

Manila Principles on Intermediary Liability (Electronic Frontier Foundation et al., 24 March 2015)

Internet Intermediaries: Dilemma of Liability (ARTICLE 19, 2013)

2012 Commission Staff Working Document on Notice and Action (see page 39) (European Commission, 11 January 2012)

La Quadrature du Net's Response to the e-Commerce Consultation (La Quadrature du Net, November 2010)

European Digital Rights' (EDRi) Response to the e-Commerce Consultation (EDRi, November 2010)

Appendix 2: Participants

Alex Agius Saliba
Member of the European Parliament

Aideen Cusack
EU Mission, Ireland

Aimilia Givropolou
Staff of Member of the European Parliament

Ajith Francis
Internet & Jurisdiction Policy Network

Alex Warofka
Facebook

Alexandra Geese
Member of the European Parliament

Alexandria Walden
Google

Alissa Starzak
Cloudflare

Amy Brouillette
Ranking Digital Rights

Athina Tsitsou
European Commission

Deborah Behar
European Commission

Bernard Shen
Microsoft

Bertrand de La Chapelle
Internet & Jurisdiction Policy Network

Birgit Sippel
Member of the European Parliament

Camille Grenier
Reporters Sans Frontières

Carlos Romero
EU Mission, Spain

Cathrin-Bauer Bulst
European Commission

Celine Grasseger
EU Mission, France

Chloe Berthelemy
European Digital Rights (EDRi)

Ciaran Shanley
Government of Ireland

Claudine Vliegen
Government of the Netherlands

Collin Kurre
BT, plc.

Courtney Radsch
Committee to Protect Journalists

Daphne Keller
Stanford Cyber Policy Center

Eliška Pírková
Access Now

Emma Llanso
Center for Democracy & Technology

Ewout van der Kleij
EU Mission, Netherlands

Francois-Xavier Dussart
Verizon Media

Frane Maroevic
Internet & Jurisdiction Policy Network

Gabrielle Guillemin
ARTICLE 19

Henk Mannekens
BT, plc.

Iain Levine
Facebook

Irene Roche Laguna
European Commission

Jana Gooth
Staff of Member of the European Parliament

Jens-Henrik Jeppesen
Center for Democracy & TEchnology

Katharina Kleine-Tebbe
Staff of Member of the European Parliament

Kirstan Fiedler
Staff of Member of the European Parliament

Krisztina Baracsi
Telenor Group

Laura Heinemann
EU Mission, Germany

Max Frey
Staff of Member of the European Parliament

Max Widmann
LinkedIn

Mira Milosevic
Global Forum for Media Development

Molly Land
Human Rights Institute at the University of Connecticut

Olga Sihmane
Telia Company

Owen Bennett
Mozilla

Patrik Hiselius
Telia Company

Prabhat Agarwal
European Commission

Raquel Carretero
Telefónica

Rebecca MacKinnon
Ranking Digital Rights

Ricardo Castanheira
EU Mission, Portugal

Richard Wingfield
Global Partners Digital

Roderik de Turck
Staff of Member of the European Parliament

Sofia Jaramillo
Staff of UN Special Rapporteur

Spandana Singh
Open Technology Institute

Andrea Fabra
Telefónica

Tom Gibson
Committee to Protect Journalists

Thomas Law
Global Forum for Media Development