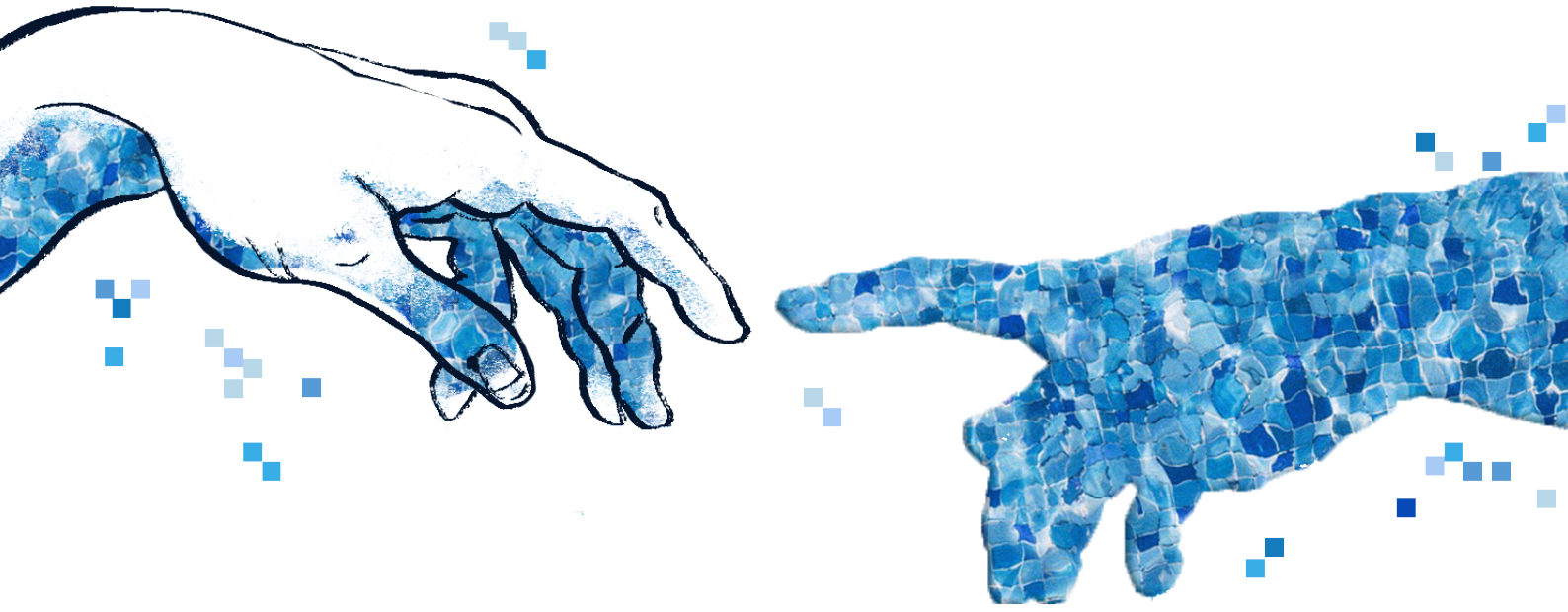
GLOBAL NETWORK INITIATIVE

Digital Trust & Safety Partnership

EUROPEAN RIGHTS & RISKS

Stakeholder Engagement Forum

Event Summary



2024

Contents

Executive Summary

The Digital Trust & Safety Partnership (DTSP) and the Global Network Initiative (GNI) brought together representatives from Very Large Online Platforms (VLOPs) and Search Engines (VLOSEs), as well as civil society and academic experts from across Europe and other jurisdictions, to discuss systemic risk assessments as provided for in the Digital Services Act. Over the course of two days of panels and workshops, participants explored DSA risk assessments and their potential impact on fundamental rights.

Key Themes & Learnings

Defining, Understanding, and Scoping Risks

Through deep dives on several risk areas (electoral processes and civic discourse, crisis and conflict-affected settings, and when harmful content becomes illegal), the Forum examined the lack of clarity on defining "systemic risks," which are often cross-border in nature and not easily scoped to the EU. Discussions also focused on the cadence and timeframe for assessments, impact on marginalised groups, data practices, and the role of other regulatory risks assessments within and outside the EU.

Assessing and Mitigating Risks While Upholding Rights

A hypothetical case study provided a jumping off point to discuss risk assessment methodologies, including how companies approach risk assessments in the absence of authoritative guidance, how they build off existing company processes, and their ability to scale and evolve in the face of new or changing risks.

Overcoming Obstacles to Meaningful Stakeholder Engagement

Participants probed the extent to which companies have been conducting stakeholder engagement in connection with risk assessments to date, considered whether and how stakeholder engagement in the context of DSA compliance requires any new practices, and imagined how civil society expertise might better inform risk assessments and mitigations moving forward.

Understanding the Impact of DSA Enforcement

Conversations touched on the enforcement of the DSA, including the potential for unintentional violations of fundamental rights through overly broad interpretation of terms and requirements.

Exploring Multiple Dimensions of the 'Brussels Effect'

The Forum highlighted several ways in which the DSA is having impacts beyond the EU. These conversations emphasised the importance of including international stakeholders, in particular experts from Global Majority countries, in conversations about the DSA.

Considering the Growing Role of AI as a Risk and Mitigation

AI was a cross-cutting theme across sessions in the Forum, with participants noting the importance and difficulties of translating systemic risks into technical systems, novel challenges assessing generative AI, and persistent concerns regarding bias in automated content moderation and other areas.

About the Forum

The Digital Trust & Safety Partnership (DTSP) and the Global Network Initiative (GNI) hosted the European Rights & Risks Stakeholder Engagement Forum on 26 and 27 June, 2024 in Brussels, Belgium. The Forum brought together over 75 attendees, including representatives from seven entities who are members of GNI and DTSP and collectively manage 13 distinct services that have been designated as Very Large Online Platforms (VLOPs) or Search Engines (VLOSEs), as well as civil society and academic experts from across Europe and other jurisdictions[1], to discuss systemic risk assessments as provided for in the Digital Services Act (DSA).

The DSA requires VLOPs and VLOSEs to assess systemic risks stemming from the design and functioning of their services and take reasonable, proportionate, and effective measures to mitigate those risks. To date, the European Commission has not provided guidance on how VLOPs/VLOSEs should identify, analyse, and assess systemic risk generally, including the methods and processes to carry out risk assessments.[2] Year One risk assessments for the first set of designated VLOPs/VLOSEs were due in August 2023 and companies are currently carrying out their year two assessments, which are due in August 2024. (See chart below for more details on timeline.)

DSA VLOP/VLOSE Risk Assessment and Audit Timeline

Date	Deliverable
April 2023	First VLOPs/VLOSEs designated by the European Commission
August 2023	Year 1 Systemic Risk Assessments due
August 2024	Year 1 Audits due Year 2 Systemic Risk Assessments due
September 2024	Year 1 Audit Implementation Reports due
November 2024	Public reports on Risk Assessments and Audits due
August 2025	Year 2 Audits due Year 3 Systemic Risk Assessments due

1 Participants included individuals based in and/or focused on the following regions: Africa, East and South Asia, Europe, Latin America, the Middle East and North Africa, and North America.

2 The European Commission has published "Guidelines for providers of VLOPs and VLOSEs on the mitigation of systemic risks for electoral processes" but these guidelines identify mitigation measures and do not cover risk assessment. See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52024XC03014&qid=1714466886277.

Risk assessment best practices highlight the importance of engaging independent experts and civil society, among others, to draw on the best available information. For example, at a high level, the OECD emphasises interactive processes of engagement, the importance of two-way communication, as well as responsive and ongoing engagement, amongst other guidance.[3]

Recital 90 of the DSA states (in part) that VLOP/VLOSEs should "ensure that their approach to risk assessment and mitigation is based on the best available information and scientific insights", including, where appropriate conducting, "their risk assessments and design[ing] their risk mitigation measures with the involvement of representatives of the recipients of the service, representatives of groups potentially impacted by their services, independent experts and civil society organisations".[4]

This Forum was designed to facilitate conversations among VLOPs/VLOSEs and a range of stakeholders with expertise in human rights, digital technologies, risk assessment processes and methodologies, and specific risk areas.

Goals

The Forum was designed to bring together stakeholders in a participatory and trusted space to provide an opportunity for input into ongoing risk assessments. Goals included:

1. Companies to share approaches and challenges related to what they are considering in ongoing risk assessment;

2. Civil society to share insights into risk assessments and risk areas; and

3. Civil society and companies to reflect on the last year of assessments as well as risk assessments and stakeholder engagement in the context of DSA going forward.

Additionally, the Forum aimed to explore how civil society expertise could inform future DSA risk assessments and mitigations. The Forum also sought to increase shared understanding of the practices and processes of assessing risks to fundamental rights, inform the implementation of this component of the DSA, and identify opportunities for companies and civil society to ensure effective regulations that protect rights online.

The Forum was intended to provide opportunities for participants to learn collectively, as well as shape stakeholder engagement within the context of the evolving regulatory regime in the EU and other jurisdictions considering similar laws. Sharing insights and perspectives across companies and civil society can improve company risk assessment and mitigation, foster additional stakeholder engagement, and help reveal unintended consequences of regulation and identify potential government overreach.

3 OECD Due Diligence Guidance for Responsible Business Conduct, available at https://mneguidelines.oecd.org/OECD-Due-Diligence-Guidance-for-Responsible-Business-Conduct.pdf

4 See the full text of Recital 90 at https://eur-lex.europa.eu/eli/reg/2022/2065/oj.

Preparation

The Forum built on discussions and learnings from DTSP and GNI's 2023 virtual workshop on "Understanding Systemic Risk in the Digital Services Act," which focused on key definitional questions, including how to define systemic risks, prioritise the four defined systemic risk areas outlined in the DSA, assess intersections between risks, and consider fundamental rights as part of risk assessments.[5] After that workshop, the organisers realised there was a pressing need for spaces to continue these conversations.

GNI and DTSP staff conceptualised the Forum's agenda, and organised and facilitated the event. Over two days, the agenda included three panels and five workshops exploring a range of topics, including: reflecting on the last year of assessments; surveying the risk landscape in Europe; undertaking deep dives into key risk areas of electoral processes and civic discourse, crisis and conflict-affected settings, and harmful content; exploring approaches and methodologies for risk assessments; and considering how the field can ensure that the DSA can support a rights-respecting ecosystem. (See Annex for the full agenda.)

In planning the agenda and facilitation, the organisers consulted their respective members, as well as outside partners, to learn more about what's working, what's not working, and where the gaps are with respect to the conduct of DSA risk assessments. In particular, the organisers closely consulted with five civil society advisors to inform the workshops, including soliciting their input to develop ideas and discussion questions and asking them to share opening remarks (see more information in the Participants section at the end of the report). Additionally, the organisers invited a wide range of expert civil society, academic, and company representatives to share "scene setting" remarks to introduce workshops and to speak on panels. Finally, the organisers sent surveys to companies and civil society participants in advance of the Forum.

The Forum was held under a modified version of the Chatham House Rule: *participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s) may be revealed; participants may note the affiliations of those that participated and are listed in the report, without attributing specific comments or positions to them*.[6]

After the event, GNI and DTSP wrote this high-level summary, which seeks to capture key learnings and takeaways from the preparation for and discussions during the Forum, within the boundaries of the modified Chatham House Rule. Prior to the publication of this summary, we made a draft available to a selected group of participants to review for accuracy and provide feedback. This summary is a result of the process facilitated independently by the organisers; it does not necessarily represent the views of DTSP's and GNI's members, nor of the individuals or organisations that participated in the Forum (see more information in the Participants annex). All participants were given an opportunity after the Forum to opt out of being listed institutionally in this report. No organisations opted out of being listed.

5 See the event summary available at https://globalnetworkinitiative.org/workshop-summary-implementing-risk-assessments-under-dsa/.

6 For more on the Chatham House Rule, see https://www.chathamhouse.org/about-us/chatham-house-rule

Google covered the costs of hosting the conference and travel for staff and civil society participants, with additional travel support provided by TikTok.

To continue the conversation and build on the learnings that emerged, GNI and DTSP will be hosting a virtual event after the first year of risk assessments have been published.

Key Themes & Learnings

Discussions during the Forum coalesced around several overarching themes: understanding risks, assessment methodologies, stakeholder engagement, DSA enforcement, the Brussels Effect, and the role of AI.

Defining, Understanding, and Scoping Risks

Conversations throughout the Forum considered the current risk landscape in the context of the challenges that have loomed large in 2023 and 2024 – including fast-evolving technological developments, like generative AI, and complex political environments during this year of elections and multiple armed conflicts around the globe – and looked forward to considering what risks might be most pressing in 2025. Focused workshops explored three key risk areas: elections and civic discourse; when harmful content becomes illegal; and crisis and conflict settings.

Key themes that emerged from the discussion included:

- **Lack of clarity on defining and scoping 'systemic risks'**: A common theme shared across stakeholder groups throughout the Forum was the lack of clarity on how to define and scope the risks identified in Article 34 of the DSA as well as how to identify when a risk should be considered "systemic." Terms such as "civic discourse", "electoral processes" and "public security" as well as qualifiers such as "foreseeable negative effect", are broad and open to wide interpretation by regulators, companies, and the public at large. Even defining "illegal content" is not yet clear under this new regulatory framework, as what constitutes as illegal is defined in other laws at either the EU or national levels. This lack of overall clarity has resulted in companies making an "educated guess" on the DSA's interpretation of systemic risks and consequently using different understandings and standards to identify and assess systemic risks (such as scope, scale, impact, severity, likelihood, and remediability). It was suggested that if companies were more transparent with civil society organisations about the categories of risks they are assessing, the mitigations they are considering, then civil society could offer insights that might help clarify definitions and could add nuance towards protecting user rights. In doing so, it is important that companies are clear how external engagement and research are informing and changing their work. The publication of year 1 reports will hopefully be an important milestone in bringing transparency into company efforts and can catalyse further exchange between companies and civil society around risk assessments and mitigation measures.
- **Accounting for context:** The context(s)in which a risk may occur matters and shapes how a company assesses, prioritises, and seeks to mitigate a risk. Contextual factors can include language, legal, political, and social environment, all of which interact differently with a platform's business model and the services and products they offer. For example, Recital 89 states that services should "take into account the best interests of minors" including "to protect minors from content that may impair their physical,

mental, or moral development." This is a contentious question where member states have different laws, which in some cases will require companies to restrict certain types of content which may be legally permitted in other jurisdictions.

- **Global and cross-border nature of risks**: Identifying risks is complicated by the requirement in the DSA to scope a systemic risk to the EU; when in practice, risks are very much cross-border in nature. For example, risks may arise outside of the EU with implications for the EU, or parts of a risk in the EU may take place outside of the EU. Similarly, EU citizens impacted by risks can be citizens of, and have family in, non-EU countries. Elections outside the EU could impact the information environment within the EU, where users also outside of the EU spread disinformation that could be consumed by users within the EU in ways that impact "civic discourse". There is also a risk of over- or under-moderation of information related to belligerents in a conflict, which may impact the information environment within the EU and potentially lead to physical harm within the EU. What part of that, if any, is or should be within the scope of the DSA? (For more on these themes, see the related section below on the "Brussels Effect".)
- **Geographic scope of risks within the EU**: There is further uncertainty on granularity - namely whether risks should be assessed at the EU or member state level and how to prioritise between these two levels. With limited resources, there is a possibility that risks within smaller countries (particularly those whose languages are not widely spoken) in the EU will be deprioritised. Relatedly, there are varying definitions of illegal content across countries in the EU, which complicates companies conducting their DSA risk assessment at the EU level.
- **Cadence of assessments**: In addition to requiring a cadence of annual risk assessments and audits of those assessments and their mitigations, Article 34 of the DSA also requires specific assessments "prior to deploying functionalities that are likely to have a critical impact on the risks identified." It's not yet clear what "critical impact" means within the context of the DSA, and therefore there is still uncertainty about how often and when additional assessments are required. So far, the regulatorily required cadence of timing for risk assessments and audits has been challenging for companies, as the internal teams who are conducting risk assessments are also involved in responding to audits, and both activities are happening at the same time each year. As a result, companies are simultaneously finalising their second assessment, while being audited on their first assessment. Additionally, other than in the context of specific Requests for Information that have been issued, none of the participating companies reported receiving feedback on their risk assessments from the Commission, so they are completing their second assessment without additional guidance. Furthermore, the teams with the necessary expertise to carry out risk assessments are also the teams who should be implementing mitigations (as well as addressing risks in non-EU contexts), putting a potential strain on time and resources.

- **Timeframes**: It is clear that for some risk areas, such as those related to elections, it is important to assess risks around a certain event (e.g. an election) or timeframe (e.g. a longer run-up period prior to and after an election), while other risk areas are ongoing - such as addressing illegal content and threats to fundamental rights. These distinct, risk-specific timeframes are important to understand and factor into related planning.
- **Impact on marginalised groups**: Risks may impact different groups unevenly, often disproportionately affecting marginalised groups. In addition, it was noted that the most marginalised groups are often difficult to identify and engage with, so additional considerations and safeguards need to be accounted for and in place when engaging.
- **Data**: There are varying types of data needed to assess risks, with varying levels of quality. The relevant data could have harmful biases embedded in them or might be incomplete or produce unclear conclusions, which needs to be taken into consideration in relation to risk assessments. In addition, collecting data related to the removal of content (including in some cases the content itself) may be necessary to iteratively improve risk assessments over time, to facilitate ongoing data analysis, synthesis of learnings, and accountability – both internally and for external researchers. Such data practices may present challenges for compliance with the EU General Data Protection Regulation (GDPR). Preservation of digital evidence for the purposes of subsequent investigation and prosecution of human rights or humanitarian abuses is especially relevant in conflict contexts.
- **Differences across platforms and services**: Risk profiles and capacities are different across companies and across services within a company. When developing guidance around risk assessments, there is a need to find the right balance between guidance tailored to a service and/or platform and guidance that can be generally applicable and serve as the basis for common standards. It is important for companies to come up with consistent frameworks so that when different teams operationalize risk assessments, they do so consistently and in ways that protect fundamental rights. Engagement with civil society can help them to identify the points of contention and prioritisation of risks to assess.
- **Balancing rights, values, and risks**: When identifying and assessing risks, companies must balance a number of conflicting issues, such as upholding the dignity of individuals vs. documentation of war crimes during times of conflict or supporting election integrity vs. protecting freedom of expression during elections. External experts can help companies in working through each situation to reach optimal solutions by bringing in additional perspectives, including considering affected stakeholders and impacts that companies may otherwise have little internal awareness of.
- **Other regulations defining risk assessments**: Other regulations within the EU (such as the EU AI Act) and outside of the EU (such as the UK Online Safety Act) have established risk assessment requirements and regulators are expected to provide further guidance on those over time. There will likely be opportunities for the Commission and others to learn from these experiences, and to provide greater clarity

on how these regimes are meant to work in relation to one another. This also presents a potential opportunity for the Commission to demonstrate leadership in building coherence across approaches to risk assessment that are emerging across contexts. The Commission must recognize that companies may rely on guidance from other jurisdictions, especially where those jurisdictions provide more detailed guidance.

Assessing and Mitigating Risks While Upholding Rights

The Forum explored risk assessment methodologies, challenges, and opportunities, including how companies have designed their risk assessment frameworks under Article 34 of the DSA. Workshops used a hypothetical case study – contributed by AlgorithmWatch – drawn from real-world scenarios as the basis for information sharing and collaborative thinking about how VLOPs and VLOSEs identify and assess risks. These workshops considered methods for identifying and classifying risk in this new environment without standard methodologies or benchmarks.

The following themes emerged from the discussion:

- **Lack of clarity on benchmarks and standards**: Similar to the lack of clarity on defining and scoping risks under the DSA, the conversation highlighted the lack of clarity on methodologies, benchmarks, and standards for risk assessments. There is no standard methodology or set of benchmarks for companies to conduct risk assessments and the European Commission has not provided any specific guidance. As a result, companies are developing their own methodologies. On the one hand, companies need flexibility given the different services they provide and contexts they operate in. However, the lack of agreed approaches has made conducting risk assessments difficult. Guidance could speak to: the level of geographic-specificity (pan-EU, by member state, or a combination approach) required for risk assessments, what qualifies as an "acceptable" threshold of risk in various contexts, what constitutes good data sets underpinning risk assessment, and expectations for stakeholder engagement related to risk assessment (e.g. issues like how structured, frequency, how it inputs into assessments). Overall, flexible guidance would give companies and stakeholders common direction, as well as a baseline to iterate against over time. It would also help establish shared understandings and facilitate more detailed and concrete discussions with stakeholders.
- **Building on existing practices**: DSA risk assessments are a compliance obligation that is, at present, often layered on top of existing processes companies already used to assess risk before rolling out products and features. Companies are building on pre-existing practices and resources such as those established through the UN Guiding Principles on Business and Human Rights, the GNI Implementation Guidelines, the DTSP Safe Framework, enterprise risk management frameworks, public transparency reporting, and risk registers. However, neither the risk assessment practitioners who are leading internal processes, nor the auditors reviewing the risk assessments, are likely to be subject matter experts on specific risks. To ensure that risk assessments help protect fundamental rights appropriately, these teams should include internal

trust and safety and human rights experts, and integrate with broader human rights due diligence processes. Companies should also ensure that risk assessments are informed by ongoing stakeholder engagement with experts and communities relevant to the risks being assessed. Appropriate resourcing, and recognition that involvement in risk assessment will have an impact on the ability of these teams to do their regular work, will also be important.

- **Scaling risk assessment practices**: Companies are working to develop and scale risk assessment practices internally to address distinct scenarios (including conflict and high-risk areas) across multiple services and teams, as well as across jurisdictions. For example, companies are exploring how to create a scalable process that works across multiple services and markets, including considering when and how to use automated processes and tools to facilitate risk assessment. Given the emergence of regulations globally that include risk assessment and other types of human rights due diligence requirements, there could be an opportunity to develop modular multi-stakeholder guidance and/or institutions, with the goal of making it more feasible and efficient for companies to comply with these regulatory frameworks while being attentive to human rights. These institutions could actively work to broaden civil society participation in risk assessments through outreach and education across contexts, languages, and sectors to ensure a diversity of perspectives and voices.
- **Evolution of risks**: Companies need to have long-term strategies in place to create scalable processes, as well as be able to respond to both immediate and evolving risks. This includes specific events, such as elections, crises, and conflicts, which could be short, medium, and long term, as well as persistent evolving concerns. For example, risks related to child sexual exploitation and abuse (CSEA) materials persist and evolve in ways that need to be assessed on an ongoing basis, as perpetrators find ways to evade mitigation measures such as hash matching and other tools. There are challenges balancing the resources (staffing & cost) that DSA risk assessments require alongside responding to immediate risks (including those occurring outside the EU). It can be difficult to align DSA cycles to agile product development cycles. To address this, needs-based critical risk assessment should be tied into annual risk assessments and external expertise should be brought onboard to help understand potential impacts and prioritise critical risks accordingly.
- **Metrics and information to inform risk assessment**: Companies vary in their approaches to considering existing internal metrics and data in their DSA risk assessments. Some companies are using existing metrics – like content rejections, appeals, and account terminations, while some are not using any internal metrics or only partially using them. Additionally, all companies who responded to the Forum preparation survey are relying on research from academics and CSOs to inform their assessments, most on news reports, and many (but not all) on engagements with stakeholders. However CSOs and academics are not always aware their work is being used in this way; more transparency about how research is used internally would

help foster more impactful relationships. Additionally, more transparent sharing of data with researchers and civil society organisations would help enable the kind of research that companies are using to support their risk assessments.

- **Financial risk concepts**: The concept of "systemic risk" comes from financial services. More research is needed to better understand lessons from the experience of risk assessments in the financial sector, as well as how risk assessments need to be appropriately adapted to the tech sector. For example, the type of risk that is assessed under the DSA is subjective and has qualitative as well as quantitative dimensions. This is different from the financial sector, where quantitative measures of risk relate to a more specific definition of systemic risk, which is predominantly focused on institution and market failure.
- **Specifics of platforms, services, and products**: It is important to consider the unique specifics of each platform, service, product, and affected stakeholder group when identifying risks and developing related mitigations. For example, what might be appropriate for a commercial social media network is not the same for a nonprofit knowledge platform, given different values and user bases. Additionally, what might work for a social media platform might not work for a search engine, given the different purposes of these products and services. This highlights the tensions between the need for flexibility, nuance, contextual specificity on the one hand, and the desire for common standards both within and across VLOPs/VLOSEs on the other hand.
- **Audits**: Although this event did not directly address audits, the role of audits and auditors came up, as audits are a critical follow-on process to DSA risk assessments as per Article 35. In addition to a lack of clarity and guidance on risk assessments, there is a similar lack of clarity, guidance, and relevant expertise related to audits as required under the DSA. This further complicates the overall picture, as auditors also need clarity to perform their assurance function. As described in the section on cadence of assessments, it is challenging that the first year audit and second year of risk assessments are happening at the same time. Companies are trying to ensure that the first assessment feeds into the second meaningfully, but they are doing that without guidance or feedback.
- **Transparency and learning over time**: ensuring these regulatory processes lead to meaningful accountability and protection of fundamental rights will be a long game, and the overarching goal should be improvement over time. The publication of risk assessment reports later this year will be one step that facilitates learning and improvement. However, those reports may not be as comprehensive as many stakeholders hope and anticipate. Participants generally acknowledged and expressed their desire for ongoing opportunities for continued learning over time beyond the annual cycle of reports. (As noted above, to facilitate further discussion and learning, DTSP and GNI will be organising a virtual follow-up event after the year one risk assessments have been published.) Additionally, other forms of transparency – like public and researcher access to data – can support better stakeholder understanding and oversight of the risk landscape.

- **Crisis protocols**: Article 48 of the DSA lays out "voluntary crisis protocols for addressing crisis situations" which are "limited to extraordinary circumstances affecting public security or public health." Given this, some companies are proactively developing their own crisis protocols, attempting to balance safety and fundamental rights, including the "foreseeable negative effect" that may be caused by conflicts outside the EU. Some participants raised concerns about how crises may draw company resources away from their regular risk mitigation activities, and potentially lead to regulatory overreach (as discussed previously). Yet, there was recognition of the value of strategic, long-term crisis planning, including applying learnings from past crises to improve the effectiveness and efficiency of responses to future crises, which could include elections.

Overcoming Obstacles to Meaningful Stakeholder Engagement

Risk assessment best practices highlight the importance of engaging independent experts and civil society, among others, to draw on the best available information. For example, at a high level, the OECD emphasises interactive processes, the importance of two-way communication, as well as responsive and ongoing engagement, amongst other guidance.[7]

Recital 90 of the DSA states (in part) that VLOP/VLOSEs should "ensure that their approach to risk assessment and mitigation is based on the best available information and scientific insights", including, where appropriate conducting, "their risk assessments and design[ing] their risk mitigation measures with the involvement of representatives of the recipients of the service, representatives of groups potentially impacted by their services, independent experts and civil society organisations".[8]

Through workshop sessions, discussion during the Forum reflected on the critical role of stakeholder engagement in risk assessments, as well as related challenges and opportunities. Participants explored how and to what extent companies have been conducting stakeholder engagement in connection with risk assessments to date, considered whether and how stakeholder engagement in the context of DSA compliance requires any new practices, and imagined how civil society expertise might better inform risk assessments and mitigations moving forward.

The following themes emerged from the discussion:

- **Challenge of low-trust environment**: Many civil society participants expressed that they feel a lack of trust in engaging with companies. They want to share their knowledge to help protect rights online, but they have often felt they were not given enough context, were pulled in different directions in their engagements, and/or were not provided with sufficient (or any) feedback on how these engagements

7 OECD Due Diligence Guidance for Responsible Business Conduct, available at https://mneguidelines.oecd.org/OECD-Due-Diligence-Guidance-for-Responsible-Business-Conduct.pdf

8 See the full text of Recital 90 at https://eur-lex.europa.eu/eli/reg/2022/2065/oj.

and their inputs were taken into account. With public reports on risk assessments not required until November 2024, many civil society experts felt in the dark about DSA risk assessment processes prior to the Forum. It became clear that insights from non-DSA specific stakeholder engagement mechanisms are at times factored into DSA risk assessments, but the consulted stakeholders were not aware of how specifically this happens. There's now a challenge of figuring out how to encourage and build trust, in order to enable productive engagement to mitigate risks and protect rights.

- **Information asymmetries**: In the context of risk assessments and mitigation measures, there are several information asymmetries between companies, auditors, regulators, and civil society that significantly hinder engagement. In particular, very few – if any – civil society members have seen a DSA risk assessment, and civil society has very little insight into what risks are being assessed and mitigated, and what actual mitigation measures are being taken by companies, such as deployment of content moderation tools, collaborations with fact-checkers, and trust and safety resources dedicated to specific languages and markets. As mentioned above, civil society participants expressed uncertainty about whether or how their inputs into broader human rights due diligence processes inform DSA risk assessments.
- **Differing expectations**: While Recital 90 offers a useful reference, it does not offer a clear process or granular expectations of what stakeholder engagement should or could look like. This has led to differences in expectations between civil society and companies on what stakeholder engagement taking place to inform a risk assessment should entail.
- **Identifying stakeholders**: To undertake stakeholder engagement around specific risks identified in the DSA, it will be important to bring relevant stakeholders into the process. Identifying who is interested and affected itself can be challenging as it needs to take into account expertise, geography, and the dynamics of specific affected communities. At a broad level, to appropriately inform risk assessment and mitigation activities, companies will need extensive input from a broad range of stakeholders, including those in Global Majority countries, vulnerable/minority groups, and digital rights experts.
- **Assuming engagement**: Often, stakeholder engagement processes assume that all stakeholders will want to be engaged, which is not always the case. There are instances when CSOs may not wish to be engaged, due to competing priorities, lack of resources, or a strategic decision to not directly engage with companies.
- **Lack of resources for civil society to engage**: Civil society organisations face resource and funding limitations that impact their ability to engage. It takes significant time to engage productively, and it can take significant funding to build evidence bases and show up at venues where research and ideas can be shared. This is worsened when aforementioned lack of clarity and transparency makes resource prioritisation harder. The field – and regulators and companies in particular – need to better consider and work to support relevant civil society activities, in order to address power differentials and structural barriers to meaningful stakeholder engagement.

- **Best practices for engagement**: The following are some of the practices mentioned that companies could adopt to improve stakeholder engagement around risk assessments:

    - To build trust, companies can be more forthcoming in what challenges they face in gathering and implementing stakeholders' feedback and create opportunities for civil society to provide feedback on concrete implementation challenges.

    - Seek engagement beyond well-known actors in order to ensure diversity and perspective (noting that the range of stakeholders that will be relevant for each service and risk may vary significantly), and beyond the annual cadence of the main risk assessment reports.

    - Be clear and transparent when and how a consultation will inform a DSA risk assessment.

    - To the extent that they have already been identified, share information about relevant risks and potential mitigation measures with CSOs *prior* to engaging with them.

    - Create a feedback mechanism to explain on what action was taken based on stakeholder feedback and when feedback could not be incorporated.

    - Create or enhance existing mechanisms for rapid feedback from CSOs in urgent situations.

Understanding the Impact of DSA Enforcement

The conversations in the workshop touched more broadly on the enforcement of the DSA, noting that the practical application of DSA is currently "experimental." While more clarity will come through experience from future assessments, the present lack of clarity and current examples of enforcement by the Commission has highlighted the potential for enforcement itself to result in the (unintentional) violation of fundamental rights. For example through enforcement actions that do not follow procedure, overly broad interpretation of terms and requirements under the DSA, and the potential for even well-intentioned interpretation and enforcement to create their own negative fundamental rights impacts.

Key themes from the discussion included:

- **Politicisation of the risk framework**: Political interference can influence and shape the interpretation of "systemic risk," particularly around newer concepts such as "civic discourse", which could politicise future enforcement of the DSA by the Commission. National Authorities – particularly in less rights-respecting jurisdictions – may politicise the risk framework and other mechanisms within the DSA. An example of how this *could* happen is reflected by the TikTok shutdown during the New Caledonia riots in May 2024; though to be clear, this specific shutdown was not connected to DSA

enforcement.[9] Obvious and egregious instances of government overreach likely will be easier for actors in the field to identify and call out. But, there is an additional risk that regulators missapply – even if in good faith – the powers granted them under the DSA, and more subtly and quietly use it to influence company practices in ways that generate benefits for particular state or non-state actors without enhancing user rights. This could be a particular risk during key democratic moments – like elections – or times of crisis.

- **Risks of enforcement as a mechanism for backdoor content regulation**: Specific to risk assessments, concerns were raised that, in practice, risk assessments could become an avenue for the Commission to enforce content regulation in a way that violates fundamental rights. For example, as both the risks articulated and the mitigation measures proposed pertain to content, enforcement related to risk assessments might lead to oppressing political speech and violation of freedom of expression.
- **Lack of transparency**: The non-public nature of discussions and conversations between government and platforms raised questions about the enforcement of the DSA becoming open to political abuse. For example, when Article 42 reports are published, mitigation mechanisms will be made public, but not conversations between the Commission and regulated companies. Therefore, there is a need to have continued forums for candid conversations between companies and non-governmental stakeholders, so they can build alliances to protect user rights. The Commission could consider making their direct interactions or guidance to companies publicly available, to mitigate the risk of political abuse.
- **Strengthening regulator capacity**: As Member States start to implement the DSA, there is a need to ensure similar levels of capacity among different regulators. For example, continued multi-stakeholder discussions and forums can enable stakeholders to share feedback with regulators and for regulators to continue to build their capacity on digital rights issues. This should include the EC, Digital Service Coordinators, as well as other regulators considering regulation focused on platform accountability. Additionally, EU Accession states – which include jurisdictions with varying levels of democratic governance and adherence to the rule of law – are considering implementing aspects of the DSA in preparation. In particular, there could be a role for civil society to engage in these contexts to offer entry points and rights-respecting policy guidance.
- **Ensuring regulator accountability**: Additionally, there is a need to ensure similar levels of accountability among different regulators. For example, regulator transparency, as described above, could be one mechanism to enable accountability. Additionally, there could be other accountability mechanisms and checks-and-balances considered to strengthen regulator accountability related to risk assessments.

9 "TikTok ban lifted as New Caledonia emergency ends," Paul Kirby, BBC News, 29 May 2024, https://www.bbc.com/news/articles/c0dd94jv9jpo

Exploring Multiple Dimensions of the 'Brussels Effect'

The conversation over the two days highlighted several ways in which the DSA is having impacts beyond the EU, i.e., the so-called 'Brussels effect'.[10] The insights from these conversations emphasised the importance of including international stakeholders, in particular experts from Global Majority countries, in conversations about the DSA.

Key themes included:

- **Export of DSA**: The mere existence of the DSA may increase the likelihood that other countries will develop their own content regulations. This includes countries without strong democratic governance, critical institutions – such as an independent judiciary or independent regulators, and relevant laws and regulations – like human rights and data protection frameworks. In such scenarios, content regulations are more likely to result in negative fundamental rights impacts. The likelihood of such an impact is increased by the Commission's proactive efforts to tout the DSA and support content regulation more broadly, such as its support for the UNESCO Guidelines on the Regulation of Digital Platforms.
- **Varying degrees of openness to the DSA**: While the Brussels effect was generally acknowledged and it was observed that some countries have explicitly or implicitly modelled aspects of their proposed regulatory frameworks on the DSA, other countries are likely to be disinclined to adopt approaches that are perceived to be European or Western. Others still may perceive the DSA to be insufficiently successful in holding companies accountable. Instead, some are intentionally pursuing models that take a different approach and form.
- **The dark 'Brussels effect'**: In practice, the DSA appears to be incentivizing covered providers to focus relevant resources on DSA compliance specifically, and on EU languages and risks more generally, which can result in a decrease in resources available to address other languages and risks, or even entire services that may be more popular or have more impact in other jurisdictions, resulting in the deprioritization of identifying and addressing risks from those contexts.
- **Learning from other countries**: It is important to learn from other countries beyond EU borders where risks have manifested and been grappled with. The Commission should ensure that its engagements on these issues is not framed as a "one-way street," but rather as opportunities for reciprocal learning and capacity building. This is even more true as the DSA, despite its variability of application around the world, will continue to be considered a benchmark legislation. Given this dynamic, it is imperative for the EU to learn from others.

10 See https://www.brusselseffect.com/

Considering the Growing Role of AI as a Risk and Mitigation

AI was a cross-cutting theme across sessions in the Forum. Key themes included:

- **Translating systemic risk into technical systems**: Translating what systemic risks means into a technical system is challenging in part because it is difficult – and at times, might not be possible – to fully understand complicated systems distributed across services and teams. This also poses challenges for assessments and audits. For instance, an auditor seeking to evaluate AI-enabled risk mitigations, may not know what it doesn't know about how the system worked previously or what alternative mitigations could have been considered. For example, a good internal technical audit of one specific system could take up to six months, and most VLOPs/VLOPSEs would be likely to have hundreds of such systems that might need to be audited.
- **Lack of methods to assess generative AI**: It is clear that AI can exacerbate online risks through aspects such as recommender systems, creation of inauthentic content, and the amplification of harmful content. Yet, - the methods to assess risks associated with AI - particularly generative AI - are currently lacking and are predominantly focused on red teaming. They are almost all designed in an ad hoc manner - reaching out to people in networks to redteam, versus gathering representative samples to test generative AI systems.
- **Challenges in automated content moderation**: A number of companies are using AI tools to automatically detect and moderate content, including as part of mitigation measures. The challenges with these tools have been well documented, including issues with accuracy that result in over or under moderation, inability to account for language and context, and inability to account for the evolving nature of expression online.
- **Impact of bias**: Algorithmic bias is pervasive and there is not a "correct way" to arrive at a perfect algorithm/outcome. Given that companies predominantly remove content automatically, even slight biases could have significant impacts on what is available online, which may contribute to systemic risk. However, it is important to distinguish between algorithmic bias and algorithmic design - e.g. understanding if there's political bias in an algorithm vs. the algorithm simply reflecting the conversation that users are having regarding a specific topic.

Conclusion

This Forum marked one step forward in the journey toward more fruitful engagement between platform companies and civil society in pursuit of the protection of fundamental rights in Europe and around the world. Representatives from digital services and civil society brought diverse perspectives to the discussion, and were able to identify points of common ground despite often opposing positions. Notably, there appeared to be opportunities for interested stakeholders to not wait for authoritative guidance from the EC, but to work collaboratively in pursuit of rights-respecting approaches to risk assessment. Forthcoming public reports on year one risk assessments and audits will provide an opportunity for shared reflection and identification of challenges and opportunities to improve the practice of assessing and mitigating risks, even if the amount of information that is disclosed through these publications may not satisfy all stakeholders. DTSP and GNI look forward to continuing this conversation through our future virtual event, and hopefully in other fora as well.

Annex I: Resources

These are some of the resources that the organisers used to prepare for the Forum, that participants shared in surveys beforehand, and that speakers mentioned during their remarks. This is not a comprehensive list, but is intended to provide a jumping off point of resources that might be useful to the various stakeholders in this space who are conducting, considering, and evaluating risk assessments.

- AccessNow: Tech and conflict: a guide for responsible business conduct (May 2023)
- Alexander Hohlfeld: Digital Services Act: Grappling with the ambiguities of disinformation. In Taming the Digital Realm. Global Content Moderation Practices (August 2023)
- Alexandre de Streel et al: A study requested by the European Parliament-Online Platforms' Moderation of Illegal Content Online (June 2020)
- Algorithm Watch: Proposals on Mitigating Election Risks for Online Platforms (March 2024)
- Algorithm Watch: Stakeholder Legitimacy Framework (February 2024)
- Alliance4Europe: Elections Incident Reports (ongoing)
- Asha Allen: An Intersectional Lens on Online Gender Based Violence and the Digital Services Act (November 2022)
- Barata, Joan, and Jordi Calvet-Bademunt: The Digital Services Act Meets the AI Act: Bridging Platform and AI Governance (May 2024)
- Barata, Joan, and Jordi Calvet-Bademunt: The European Commission's Approach to DSA Systemic Risk is Concerning for Freedom of Expression (October 2023)
- BSR: Effective Engagement with Technology Companies - A Guide for Civil Society (May 2024)
- BSR & Just Peace Labs: Conflict Sensitive Due Diligence for ICT Companies: Guidelines & Toolkit for Human Rights Practitioners (2022)
- CDT: Fostering responsible business conduct in the tech sector – the need for aligning risk assessment, transparency and stakeholder engagement provisions under the EU Digital Services Act with the UNGPs (August 2023)
- CERRE: Cross-Cutting Issues for DSA Systemic Risk Management: An Agenda for Cooperation (July 2023)

- CERRE: Systemic Risk in Digital Services: Benchmarks for Evaluating the Management of Risks to Electoral Processes (May 2024)
- DSA Observatory (et al): The DSA and Platform Regulation Conference (February 2024)
- DTSP: The Safe Framework Specification (July 2024)
- ECNL & Access Now: Towards Meaningful Fundamental Rights Impact Assessments Under the DSA (September 2023)
- ECNL: Framework for Meaningful Engagement
- EPD: Identifying systemic risks for civic discourse and electoral processes and related mitigation measures under the EU's Digital Services Act (January 2024)
- EU Code of Conduct on Countering Illegal Hate Speech Online
- EU COMMISSION RECOMMENDATION 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online (March 2018)
- GNI & DTSP: Implementing risk assessments under the Digital Services Act (June 2023)
- GNI, ICRC, & SIPRI, Exploring Tech Company Responsibility in Conflict (May 2024)
- GNI & GPD: Engaging Tech Companies on Human Rights (October 2022)
- GNI: Ensuring Digital Services Act Audits Deliver on Their Promise (February 2024)
- Meta: Guide for conducting inclusive stakeholder engagement (February 2024)
- Mozilla: Navigating the Digital Services Act: exploring key elements and scenarios (October 2023)
- NDI: Digital Responses to Crises: An Action Plan for Platforms and CSOs Confronting Online Threats (October 2023)
- OECD: Due Diligence Guidance for Responsible Business Conduct (especially pp. 49-51 sections on Meaningful Stakeholder Engagement)
- Ranking Digital Rights: Methods and Standards
- UN Guiding Principles on Business and Human Rights (UNGPs) (especially pp. 19-20, Principle 18)
- UNICEF: Child Rights Impact Assessments in Relation to the Digital Environment (April 2024)
- U.S.- EU Trade and Technology Council (TTC): Joint Principles on Combating Gender based Violence in the Digital Environment (April 2024)
- Wikimedia Foundation: Child Rights Impact Assessment (January 2024)

Annex II: Participants

Representatives from the following organisations attended the Forum.

The findings, interpretations, and conclusions expressed in this document are a result of the process facilitated by the Global Network Initiative and the Digital Trust and Safety Partnership. They do not necessarily represent the views of the participating organisations, nor the entirety of their members, partners, or other stakeholders. Participants attended under a modified version of the Chatham House Rule. The comments and observations in this document reflect our understanding of the interventions made during the discussion and should not be attributed to any individual participant.

Academia

- Annenberg Public Policy Center at the University of Pennsylvania
- Institute for Data, Democracy & Politics (IDDP) at George Washington University
- Vrije Universiteit Brussels
- Alexander von Humboldt Institute for Internet and Society (HIIG)
- Centre for Communication Governance (CCG) at National Law University Delhi
- Centro de Estudios en Libertad de Expresión (CELE) at University of Palermo
- Oxford University
- Sciences Po Law School
- St John's University
- Stanford Law School
- University College London
- University of Amsterdam, Institute for Information Law, DSA Observatory
- University of East Anglia

Civil Society and International Organisations

- 7amleh
- Access Now
- AlgorithmWatch*
- Alliance for Europe
- Article 19*
- Atlantic Council
- BSR

- Center for Democracy and Technology (CDT) Europe*
- Centre on Regulation in Europe (CERRE)
- Electronic Frontier Foundation (EFF)
- European Center for Not-for-profit Law (ECNL)*
- European Partnership for Democracy (EPD)
- Future of Free Speech
- Global Forum for Media Development (GFMD)
- Global Partners Digital
- Humane Intelligence
- Independent*
- International Center for Not-for-profit Law (ICNL)
- Internews
- Liberties
- LIRNEasia
- Mozilla Foundation
- National Democratic Institute (NDI)*
- Paradigm Initiative
- Search for Common Ground
- TechFreedom
- The Global Disinformation Index
- WeProtect Global Alliance
- WITNESS
- World Benchmarking Alliance
- International Committee of the Red Cross (ICRC)
- UN Human Rights (OHCHR)

**Denotes that representative from the organisation served as a civil society advisor to one of the Forum's workshop sessions, helping to develop ideas and discussion questions, as well as reviewing this report prior to publication.*

Companies / Platforms

- Apple
- Google
- LinkedIn
- Meta
- Microsoft: Bing
- Pinterest
- TikTok
- Wikimedia Foundation

About the Organisers

GNI

GNI is the leading multistakeholder forum for accountability, shared learning, and collective advocacy on government and company policies and practices at the intersection of technology and human rights. We set a global standard for responsible company decision-making to promote and advance freedom of expression and privacy rights across the technology ecosystem.

DTSP

The Digital Trust & Safety Partnership is a unique initiative focused on promoting a safer and more trustworthy internet. We are committed to developing, using and promoting industry best practices, reviewed through internal and independent third-party assessments, to ensure consumer trust and safety when using digital services.

Annex III: Agenda

DAY 1: WEDNESDAY, 26 JUNE

Part 1: Introduction, Reflections, and Scene Setting

8:30 Light breakfast available & Badge pickup

9:30 - 10:00

Welcome

Plenary remarks from the organisers

10:00 - 11:00

Panel: Conducting risk assessments in practice: looking back & forward

As this second year of assessments wraps up, we open the Forum with a high-level session reflecting on how risk assessment is happening in practice. The DSA requires VLOPs/VLOSEs to assess systemic risks stemming from the design and functioning of their services and take appropriate measures to mitigate those risks, identifying a set of risks for companies to assess and providing a list of possible mitigation measures. Yet, there is little guidance on how VLOPs/VLOSEs should identify and assess systemic risk, including the methods and processes to carry out risk assessments. The first year of risk assessments were due in August 2023 and companies are currently carrying out their second year of assessments, due in August 2024. This panel sets the table for looking back to 2023 and the first half of 2024 to reflect on practice so far, and looking forward to the rest of 2024 and 2025 to imagine how processes might improve based on lessons learned.

11:00 - 11:15 Coffee break

Part 2: Deep dives into thematic risks and their mitigations

11:15 - 12:00

Panel: Reflecting on the risks & rights landscape in Europe and around the world

This panel sets the table for exploring the landscape of systemic risks to individuals and society across Europe. Over the last year and a half, Europe and the world have seen many challenges and risks to human rights, from conflict and crisis, elections, impacts of online extremism, hate, and harassment. Digital platforms continue to both support human rights and pose risks to them.

The panel will consider the current risk landscape in the context of the challenges that have loomed large in 2023 and 2024 – including fast evolving technological developments, like generative AI, and complex political environments during this year of elections and multiple armed conflicts around the globe – and look forward to consider what risks might be most pressing in 2025.

11:00 - 11:15 Lunch

12:45 - 2:15 Concurrent Workshops

**Three separate workshops will run on the following topics concurrently. We have assigned participants to attend one of these based on expressed interest and our best attempts to ensure a balance across sectors, expertise, geographies, etc. See discussion questions in attached pre-reads.*

WORKSHOP: Electoral processes and civic discourse

In 2024, at least 64 countries, along with the European Union, will hold a national election, the outcomes of which will significantly impact individuals and societies and their rights online and offline. The ecosystem around the creation of content, including that related to civic discourse and elections, as well as its dissemination, promotion and consumption is complex. Experiences over the past decade have demonstrated the increasingly central role that digital technologies and online platforms play in elections and civic discourse. Platforms facilitate communication, enable access to information, and can streamline processes. Yet, there are numerous risks related to digital platforms and elections, such as interference with elections and civic discourse through aspects like online harassment, disinformation, the manipulation of content and subsequently voters, opacity around political advertisements, and the misuse of personal data.

The protection of integrity of elections has been noted by the European Commission as one of the key priorities of enforcement of the DSA. Along these lines, Article 34 lists actual or foreseeable negative effects on civic discourse and electoral processes, and public security as a specific risk that companies must include in their assessments of systemic risks. In March 2024, the European Commission published guidelines on recommended measures VLOPs and VLOSEs could take to mitigate systemic risks online that may impact election integrity, such as reinforcing internal processes, implementing measures tailored to specific election periods and local context, adopting mitigation measures linked to generative AI, cooperating with stakeholders including civil society, adopting incident response mechanisms during an electoral period, and assessing the effectiveness of measures.

WORKSHOP: When Harmful Content Becomes Illegal:
Mitigating Risks While Protecting Rights

Certain harmful online behaviour and content is now illegal and/or criminalised under EU laws and regulation, such as the EU Directive to combat violence against women and domestic violence and the EU Code of conduct on countering illegal hate speech online. For example, as CDT raised recently, EU law criminalises or is considering criminalising non-consensual sharing of images; cyber stalking; cyber harassment, and cyber incitement to hatred. This shift to defining further categories of illegal content can pose concerns to freedom of expression and other rights. The issue is especially complex as the definition of these harmful categories are not clear-cut.

Through facilitated full and small-group conversations, this session will foster a discussion on how civil society and practitioners might think about content areas that straddle from harmful to illegal; they require risk assessment, but also might be illegal. How can civil society and practitioners consider assessing and mitigating risks at those intersections and thresholds in a rights-respecting way?

WORKSHOP: Crisis & Conflict-Affected Settings

Online platforms play an important and complicated role during times of crisis and conflict. On one hand, they may offer critical civilian functions and facilitate information sharing and documentation, yet they can also be used for military functions and be misused to harm civilians and prolong conflict. The impact of online harms such as disinformation and hate speech are further exacerbated during times of conflict, deeply impacting the rights of individuals and communities. As such, conflicts involve distinct risks and vulnerabilities for companies, their customers, and others who may be impacted by their activities. As multiple conflicts have emerged and deepened across the globe this year, online platforms need to understand both the applicability of international human rights law and international humanitarian law to ensure they are identifying and addressing the unique needs of vulnerable people and populations. Additional and specific decision-making criteria and risk-analysis tools in the form of enhanced due diligence is also needed for operations in conflict settings. This session will explore questions around risk assessments during times of conflict such as what does enhanced due diligence for conflict settings look like in the context of the DSA? And when and how should International Human Rights Law/Law of Armed Conflict be relevant to the identification of risk mitigation measures under Article 35?

2:15 - 2:30 Coffee break

2:30 - 3:00

Facilitated sharing from workshops

DTSP and GNI organisers will facilitate sharing high-level reflections from prior workshops.

3:00 - 4:30

Concurrent Workshops

Making Stakeholder Engagement in Risk Assessments Meaningful

**Three separate workshops will run on this same topic concurrently, across three rooms.*

This session will begin in plenary, with scene-setting remarks from participants, who will provide overarching reflections on stakeholder engagement, challenges, and opportunities.

Risk assessment best practices and Recital 90 of the DSA highlight the importance of engaging independent experts and civil society, among others, in order to draw on the best available insights about systemic risks, online platforms, and the European context. Yet, while Recital 90 offers a useful stepping off point, it does not offer a clear process or really granular expectations of what stakeholder engagement should or could look like.

As this second year of VLOP/VLOSE risk assessments wrap up, we have the opportunity to reflect on how companies have been conducting stakeholder engagement in connection with their risk assessments so far, consider whether and how stakeholder engagement in the context of compliance requires any new practices, and imagine how civil society expertise might better be able to inform risk assessments and mitigations moving forward.

We hope to build on GNI and DTSP's experience as multistakeholder conveners and Forum participants' experience designing, hosting, and participating in stakeholder engagement to further discuss what meaningful stakeholder engagement over time could look like to inform DSA risk assessments.

Key questions include:

- How is stakeholder engagement around risk assessments happening in practice?
- Is stakeholder engagement within the context of compliance different? If so, how?
- What suggestions do each sector have for how to best engage each other in relation to DSA risk assessments?
- How should stakeholder engagements be fed into assessment?
- How might we collectively develop mechanisms to build trust and encourage engagement and, where appropriate, information sharing across sectors towards shared goals to mitigate risks and protect fundamental rights?

4:30 - 4:45 Break

4:45 - 5:30 Facilitated sharing from workshops

DTSP and GNI organisers will facilitate sharing high-level reflections from prior workshops, conclude the day, and tee up the program for day two.

5:30 - 6:30 Happy Hour

Please join us for happy hour and light appetisers.

DAY 2: THURSDAY, 27 JUNE

8:30 Light breakfast available & Badge pickup

Part 3: Process and methods for assessing systemic risks to fundamental rights

9:00 - 9:30

Welcome

Plenary remarks from the organisers

9:30 - 11:30

Concurrent Workshops

*Three separate workshops will run on this same topic concurrently, across three rooms.

This session will begin in plenary, with scene-setting remarks from participants, who will provide overarching reflections on risk assessment methodologies, challenges, and opportunities. It will be followed by concurrent workshops that will use a hypothetical case study drawn from real-world scenarios as the basis for information sharing and collaborative thinking about how VLOPs and VLOSEs are identifying and assessing risks.

These concurrent workshops will delve into how companies have thought about designing their risk assessment frameworks under Article 34 of the DSA, including methods for identifying risks and classifying risk, in this new environment without standard methodologies or benchmarks.

Key questions include:

- How might the developments presented in the scenario affect your risk assessment approach?
- What are key questions you would need to ask to get necessary information for your risk assessments and how would you answer them?
- In light of the workshop discussions on stakeholder engagement, how would you involve external expertise in your risk assessment under these circumstances?
- Risk prioritisation: given the scenario, what sort of risks could be most severe and probable?

11:30 - 12:00

Facilitated sharing from workshops

DTSP and GNI organisers will facilitate sharing high-level reflections from prior workshops.

12:00 - 12:45 Lunch

12:45 - 1:45

Panel: Towards a rights respecting digital ecosystem

The effectiveness of risk assessments under the DSA depends on several factors. This includes how assessments are used to inform understanding, identifying, and responding to different risks in an ongoing and meaningful way across the digital ecosystem. To make risk assessments effective, stakeholder groups – including civil society, companies, and regulators – need to have appropriate mechanisms to share lessons and learn from each other. These lessons also need to be able to appropriately inform and be informed by other mechanisms under the DSA, such as audits, transparency reporting, sharing of data for research purposes, and crisis protocols, so that the DSA is able to create a rights-respecting ecosystem of accountability.

1:45 - 2:15

Thank You & Wrap Up

DTSP and GNI organisers will conclude the program.

2:15 - 3:00 Coffee Reception