GLOBAL NETWORK INITIATIVE

Digital Trust & Safety Partnership

European Rights & Risks: Stakeholder Engagement Forum 2025

EVENT SUMMARY

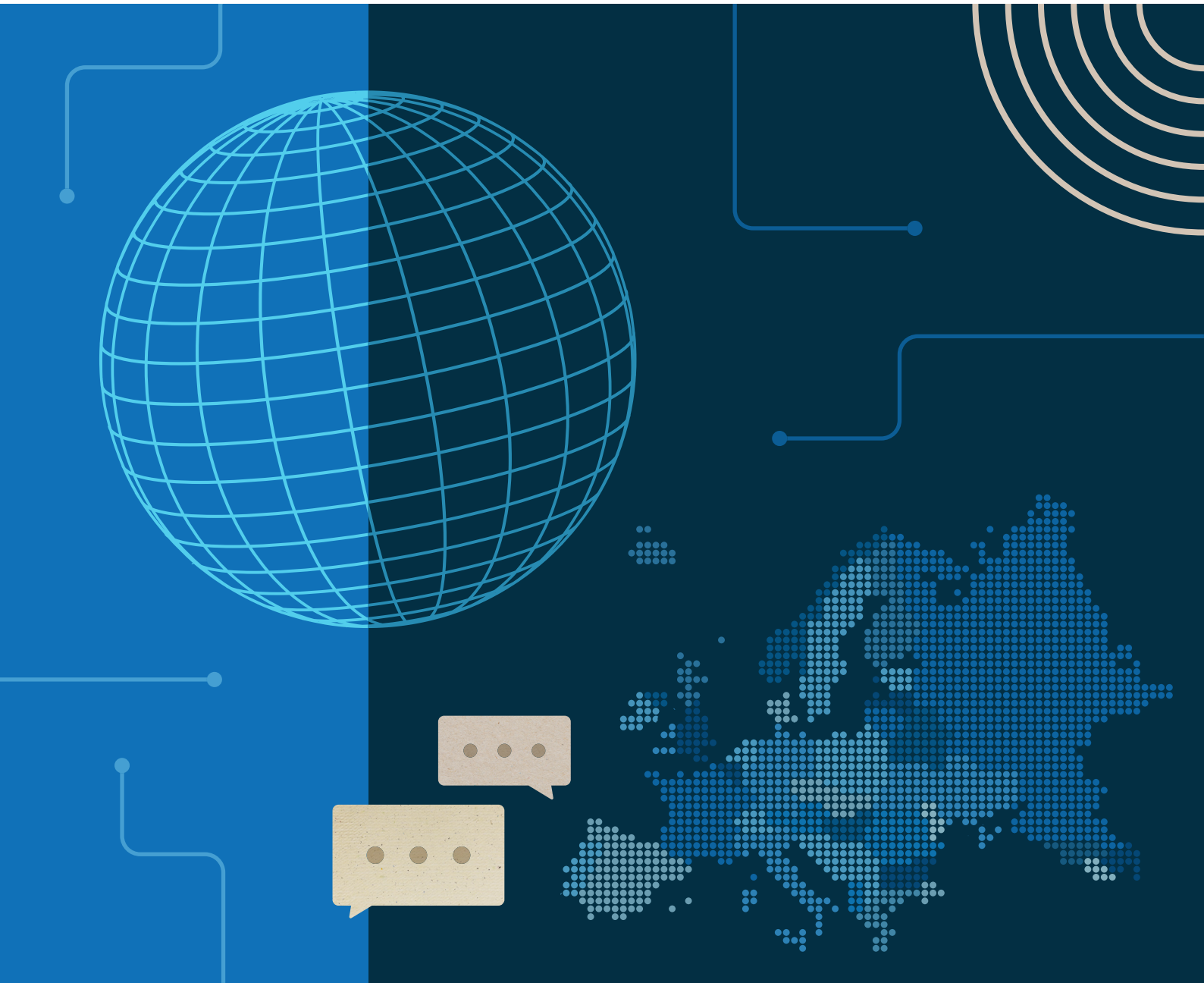

Table of Contents

Executive Summary

The Digital Trust & Safety Partnership (DTSP) and the Global Network Initiative (GNI) both work to foster responsible business conduct in line with international human rights values. Our memberships, missions, and methods are distinct but overlapping, which allows us to find synergies and bridge gaps.

For three years, DTSP and GNI have been bringing experts together across stakeholder communities to discuss implementation of the EU Digital Services Act's (DSA) risk management provisions, which are closely related to our respective frameworks in their focus on fundamental rights and proportionate and effective risk management. Each new convening has built off of the insights and relationships fostered in the last one; the themes and recommendations summarized here and elaborated on in the full report are also cumulative.

Key Themes

1. **Embedding human rights-based approaches to assessment, mitigation, and enforcement.** Companies that have adopted human rights-based approaches can deepen their implementation; others can benefit from using human rights approaches to ground and guide the practice of risk assessment and mitigation. To ensure rights-based approaches, it is critical that external stakeholders scrutinize the overall regulatory implementation to guard against both ineffective implementation and overly broad or politicised interpretations or enforcement.

2. **Focusing on how product design interacts with platform functionality and mitigation strategies.** More engagement on the interplay between risks, mitigations, and product design, particularly how design can both create and mitigate risks, could significantly improve risk assessments. This needs to be tailored to the specifics of each platform's function and features.

3. **Integrating stakeholder insights on risk areas and mitigations, particularly in terms of proportionality.** All actors need to more holistically consider the design of mitigations in their specific risk context for the possibility of unintended and disproportionate impacts on rights.

4. **Using data and metrics to show validity, effectiveness, and improvement over time.** Civil society organisations are still not sure which risks are most prevalent, or what data went into determining risk levels. Comparability across the reports, when it is practical, can enable more of an ecosystem level understanding of risks and approaches to mitigations.

5. **The need to address persistent tensions in meaningful stakeholder engagement.** Asymmetries between civil society and companies in stakeholder engagement remain, and in some circumstances have heightened over the last year. A window of opportunity exists to define this regulatory system, underscoring the critical importance of fostering meaningful and productive engagement across regulators, companies and civil society.

6. **Understanding the perceived and actual role of DSA audits with regard to risk assessment and mitigation.** Differing conceptions of the role of audits and auditors can exaggerate communications and expectations gaps.

7. **Seeking rights-respecting coherence of risk-based online regulatory frameworks.** Company and civil society stakeholders have identified that further guidance on the definition of systemic risk, benchmarks, and metrics, would improve the practice of DSA risk assessments, but there is not yet a clear picture of what kind and level of guidance would make risk assessment effective, rights-respecting, comprehensive, coherent, and potentially comparable. In the absence of definitive regulatory guidance from the European Commission, platforms are looking to guidance from other regulators, stakeholders, and frameworks.

About the Forum

On 3 and 4 June, the Digital Trust & Safety Partnership (DTSP) and the Global Network Initiative (GNI) hosted the *2025 EU Rights & Risks: Stakeholder Engagement Forum* on assessing systemic risks while protecting fundamental rights under the Digital Services Act (DSA) in Brussels, Belgium.

This was the second annual in-person edition of the Forum, informed by an interim virtual convening held in January 2025. The Forum brought together more than 75 attendees, including representatives from eight service providers who are members of GNI and DTSP and collectively manage 14 distinct services that have been designated as Very Large Online Platforms (VLOPs) or Search Engines (VLOSEs). The event also featured participation from civil society and academic experts from across Europe and other jurisdictions. Participants came together to discuss systemic risk assessments as provided for in the DSA. The organisers deeply appreciate the participants' time and insights.

Context

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. At the time of the Forum, many VLOPs and VLOSEs were in the process of carrying out their third round of systemic risk assessments, most of which are due to the European Commission in August 2025 and will be published in November 2025. While the Forum was focused on the DSA, the discussion acknowledged and referenced the existence of other, relevant regulatory regimes with similar risk assessment and mitigation requirements.

This was the first in-person convening held after the publication of the first round of VLOP/VLOSE risk assessments, mitigations, and associated audits. It took place in the wake of significant transatlantic geopolitical shifts, with ongoing impacts on the tech policy landscape and the stakeholders that work within this space.

Amidst this changing environment, Forum participants took stock of how the DSA regulatory framework is working and what can be improved. Over two days, the agenda included three plenary panels and seven break-out workshops (see Annex III for the agenda).

Across these sessions, participants focused on:

- Assessing risks in relation to platform type and product design;
- Understanding the impacts of government actions (and inaction) throughout the regulatory framework;
- Considering the appropriateness, proportionality, and effectiveness of mitigations;
- Working towards DSA risk assessments serving as ongoing learning exercises;
- Centering the protection of fundamental rights throughout these endeavors; and
- Better engaging stakeholders and incorporating received input throughout risk assessment and mitigation processes, and on an ongoing basis.

While the Forum represented a key opportunity to participate in and shape stakeholder engagement in the developing space of DSA risk assessments, the organisers made clear that we expect participating companies to build on their participation by conducting their own stakeholder engagements. The organisers believe companies should undertake a range of engagements – which vary in form, and with a range of stakeholder groups and types of expertise – across their products and services.

Goals

The organisers articulated the following objectives in advance of the Forum:

- Companies share information with civil society about how companies assess and mitigate risks in relation to platform type and product design.
- Civil society experts share analysis, questions, and recommendations with companies that could inform rights-based risk assessment and mitigation measures.
- Collectively take stock of how the overall regulatory framework on risk assessments is working, what has been achieved, and whether it is protecting the rights and safety of users.
- Collectively brainstorm what actors across the field could do to help enable risk assessments to center rights-based approaches and be ongoing learning exercises.

Terms of Engagement and Preparation

GNI and DTSP staff conceptualised the Forum's agenda, and organised and facilitated the event. In planning the agenda and facilitation, the organisers consulted their respective members, as well as outside partners, to learn more about what is working, what is not working, and where the gaps are in how companies are conducting DSA risk assessments. In particular, the organisers closely consulted with numerous civil society experts to inform the agenda. 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.

The Forum was held under GNI and DTSP's respective Antitrust Policies and GNI's Code of Conduct. It was also 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.*

After the event, GNI and DTSP wrote this high-level summary, which seeks to capture key themes, learnings, and recommendations from the 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 for a review for accuracy. 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 list of participants in Annex II). All participants were given an opportunity after the Forum to opt out of being listed institutionally in this report; no organisations opted out.

The Forum was hosted at Google's office in Brussels. Financial sponsors were Google, Meta, Microsoft, and Tiktok, who covered the costs of hosting the conference and staff and civil society travel. The Oversight Board provided additional travel support for civil society.

Key Themes, Learnings, and Recommendations

The following sections are drawn from insights shared on plenary panels and during break-out workshops. The panels covered recent developments in DSA risk assessments; enabling deeper shared learning and more rights-based assessments; and imagining a rights-respecting future. The workshops addressed risks, mitigation measures, and protecting fundamental rights in the context of platform type; better assessing risks and tailoring mitigation measures while protecting fundamental rights; and enabling shared learning and rights-based assessments. See Annex III for the agenda.

01 Further embed human rights-based approaches to assessment, mitigation, and enforcement.

Key learnings

- **As a result of what was published in the risk assessment reports, there is some emerging understanding about how companies are defining "systemic risks".** However, the term "systemic risk", which has been persistently identified as lacking definition in ways that could negatively impact rights, continues to not be clearly defined within the DSA's regulatory framework.

- **Some companies are already building on experience and expertise gained from implementing human rights frameworks,** like the United Nations Guiding Principles on Business and Human Rights (UNGPs), the OECD Guidelines on Multinational Enterprises (OECD Guidelines), the GNI Principles on Freedom of Expression and Privacy and their Implementation Guidelines (GNI framework), and other relevant approaches. This includes incorporating existing human rights due diligence (HRDD) and impact assessment (HRIA) practices into DSA risk assessment (and vice-versa).

- **However, there are concerns that the language and framing of "risks", as opposed to rights, can obscure the need to ground these assessments in human-rights**

approaches that seek to protect users rights. Additionally, the framing of risks adopts the language of "regulatory compliance," as opposed to the language of human rights, which can be disempowering for civil society, the general public, and other actors who are not specialists in compliance.

- **There are gaps in how companies are identifying risks to user rights in their risk registers,** which are tools that document and serve as an internal repository of identified risks. Risk registers are valuable approaches, as they give companies a base and set of standard risks to evaluate over time. It's particularly helpful when these registers are shared externally in the reports. Some companies could more explicitly identify risks to a range of user rights in their registers; they could also better identify risks *from* state actors.

- **It is critical that external stakeholders scrutinize the overall regulatory implementation to guard against both ineffective implementation and overly broad or politicised interpretations or enforcement.** This means scrutinizing how companies are conducting their risk assessments and how government actors are positioning and enforcing the regulatory framework. To do this effectively, at a minimum, civil society and academia need access to relevant data from companies and regulators, as well as resourcing.

Recommendations

- **Companies should adopt or more comprehensively adopt human rights-based approaches as the underlying framework for assessing and mitigating risks.** International human rights frameworks, principles, case law, and scholarship offer existing instruments and shared language that can provide guidance to help define the new terminology of "systemic risk" introduced by the DSA and inform the development of mitigation measures. This can enable a rights-respecting approach, and work to build coherence across company assessments. Several companies are already taking this approach, which can be further strengthened. Companies should be transparent and share learnings about these efforts.

- **Companies should use their DSA-related risk assessments to inform, formalize, and strengthen broader human rights due diligence efforts.** There may be risks not explicitly prescribed in the DSA that could be relevant and included in companies' assessments. Companies should also more explicitly identify risks to a range of user rights, including from state actors, in their risk registers, if they don't already.

- **Companies should explain which risks were considered but not included in their published assessment reports, and why, as well as if they are considered in other due diligence efforts,** so external stakeholders can understand how companies evaluated the salience of risks, what was considered not relevant – either to the platform or in the context of the DSA – versus not evaluated, and then offer feedback.

- **Civil society should continue to research, to build on the existing guidance already produced, and to further clarify how companies can more comprehensively apply human rights approaches in their risk assessment methodologies and due diligence frameworks.** This could include further recommendations for the types of transparency, data, and benchmarks needed to enable accountability.

02 Increase focus on product design, risks, and mitigations in the context of platform function.

These insights came from three concurrent workshops covering: (a) search engines and knowledge platforms, (b) social media platforms, and (c) app stores and marketplaces. This section includes cross-cutting learnings, session-specific learnings, and related recommendations.

Cross-cutting learnings

- **Risk assessments need to be tailored enough to consider the specifics of each platform,** as platform functions and features are different. For example, search engines, social media platforms, and app stores serve very different functions and therefore risks will present differently and need to be mitigated differently.

- **Mitigations should be tied to an identified risk.** Some mitigations were not connected to risks within reports. And even where mitigations were tied to risks, it was often hard to understand the connection within the reports.

- **Civil society and researchers noted that it is very hard to parse the reports.** For example, the report structures are complex, they are quite long, sometimes they are not designed for readability, some references required clicking through many links or links were broken, often they are not machine readable, along with other concerns.

Key learnings

A. SEARCH ENGINES & KNOWLEDGE PLATFORMS

- **In conducting and evaluating risk assessments for search engines, it is important to recognize that their functional purpose is to provide information that is responsive to user queries.** As such, respect for the right to access information is particularly critical, in the context of respecting freedom of expression.

- **More information to better understand how risk assessments and mitigations are addressing the evolving nature of search engine products would be helpful,** especially in relation to new product integrations featuring generative AI.

- **The published reports reflected a lack of clarity in how the regulatory framework categorises Very Large Online Search Engines (VLOSEs),** which are designated separately from Very Large Online Platforms (VLOPs). How to understand and address the integration of AI into different services was a consistent theme, with particular attention paid to how AI is changing the nature of search. *(Organiser note: this lack of clarity also arose in planning the Forum's workshop discussions, as it was not clear how to categorise different platforms. We decided to include the Wikimedia Foundation alongside search engines in this workshop, hence the use of "knowledge platforms" in the title even though that is not a term in the regulatory framework.)*

- **There are risks at the intersections and links between platforms that are often under-addressed, and could be discussed further in stakeholder engagement, in part to clarify where responsibilities lie.** For example, a platform may receive notice from a search engine that content has been delisted related to the right to be forgotten. The impacts on freedom of expression of such a delisting may be judged differently by each service. In another scenario, the decision to downrank certain content on a platform may echo in that same content's ranking by a search engine. There is a need for anchors and methods that practitioners can use to look at the cross-platform "systemic" nature of these risks, as they are happening across the online ecosystem. While included in some risk assessment reports, it will be useful for companies to comprehensively include when and how they resolve such tensions and trade-offs.

- **More information to better understand the risks and mitigations related to the intersection of influencing factors (identified in Article 34.2), such as advertising, in relation to search results would be useful.** There is a difference between "organic"

search results versus advertising, and how an advertising product works is different from how organic search works, which shapes associated risks and mitigations.

- **In considering risks and designing mitigations related to search engines, there are under-explored tensions between respecting user privacy, ensuring product quality, and enabling user control.** For example, mitigations designed to reduce risks to user privacy could also be perceived as having negative impacts on access to information, so there is a persistent balancing that's needed. User control can be one way to navigate these trade-offs, but this can come into tension with quality of the service.

B. SOCIAL MEDIA PLATFORMS

- **More engagement on the interplay between risk and social media product design, particularly how design can *both* create and mitigate risks could significantly improve risk assessments.** The first round of reports included a wide range of risks and possible accompanying mitigations; overall though, there seemed to be more focus on risks related to user-generated content rather than risks related to product design. For example, only a few companies explicitly identified how their features and designs could create harms (such as behavioral addiction in children), and outlined related mitigations; most companies simply outlined their mitigations.

- **There was a perceived lack of information in the first round of reports on social media risks related to recommender systems.** While it was acknowledged that recommender systems are sensitive for companies in terms of competitive concerns, stakeholders hope that more data and information can be shared publicly about possible risks and mitigations. For example, civil society would have liked to better understand the level of efficacy for recommender systems that has been revealed through internal experiments by platforms (e.g. have platforms tried multiple algorithms and preferred one over the other because of fewer harms or other metrics?).

C. APP STORES AND MARKETPLACES

- **In the first round of reports, key risk categories included** the potential for app stores to facilitate access to apps that might host child sexual abuse material (CSAM) and terrorist content; apps and merchandise facilitating scams & fraud; malicious apps; apps with content promoting harmful practices and gender-based violence; and age-appropriate apps (e.g. age gating), etc.

- **Risks and rights frameworks apply to end users *and* also to: upstream actors such as app developers** (in the case of app stores), **as well as sellers and traders** (in the case of marketplaces); **and broader, downstream affected communities** (e.g. users impacted by app content, product offerings, or moderation decisions).

- **The types of mitigations available to app stores and marketplaces can be blunt, so it is particularly important to consider the proportionality of mitigations for risks related to these product categories.** For example, stakeholders agreed that removing an app is largely a disproportionate measure for an app store to take, except in specific high-risk categories like CSAM. There are other measures that can be further explored that could reduce overmoderation, like the existing appeals process, remedial timeframes, user education to increase digital literacy, and tools for users to customize their experiences.

- **Risk assessments could better consider the human rights obligation for app stores and marketplaces to consider the proportionality of government ordered app blocking,** as blocking apps can lead to blocking access to essential services. When considering blocking or taking down an app, companies can conduct a human rights impact assessment that explicitly evaluates the potential consequences for developers (e.g., loss of livelihood, censorship) and users (e.g., loss of communication, access to critical services, information, or even economic activity). Where feasible, these HRIAs should include engagement with relevant stakeholders. When apps are blocked or taken down, more detailed information and reasoning could be shared in transparency reports.

- **There could be further discussion between company practitioners and civil society about the risks from product design, particularly addictive designs; and the risks from in-app purchases, particularly to consumers and minors.** More work is needed to better articulate the responsibilities of marketplaces in these contexts.

Cross-cutting recommendations

- **Companies and civil society organisations should consider the specific designs and features of the platforms they are assessing or researching, and the full range of impacted stakeholders.** Risk assessment could be made more effective by focusing more on risks from and mitigated by product design. In particular, companies should seek to disclose more on risks related to recommender systems, without sharing

competitive information. Tying to the need for better metrics, there is an opportunity for convergence around expected metrics for recommender systems.

- **Companies should make the assessment reports more legible.** While they are first designed for regulators, and therefore must be comprehensive, there are additional key audiences like civil society and researchers who would benefit from easier readability. This could include improved design, making the reports machine-readable where possible, noting more clearly the purpose of different parts of the report, and fixing broken links.

- **Companies and civil society organisations should consider more specific focus on risks related to advertising products, monetization, and in-product purchases.**

- **Companies should consider a wider range of mitigation measures – including design changes, awareness-raising measures for users, and enabling user control – with clearer descriptions of the tensions between rights and principles.** In doing so, it is particularly useful to describe under-explored tensions, such as in relation to increasing user control. Civil society organisations can then share more specific thinking on making trade-offs to balance these tensions.

03 Better integrate stakeholder insights on risk areas and mitigations, particularly in terms of proportionality.

These insights came from three concurrent workshops covering: risks of gender-based violence in relation to product design, risks of terrorist and violent extremism content in relation to product design, and the draft guidelines on the protection of minors online under the Digital Services Act in relation to child rights assessment best practices. This section includes session specific learnings and cross-cutting recommendations.

Key learnings

A. RISKS OF GENDER-BASED VIOLENCE IN RELATION TO PRODUCT DESIGN

- **In the first round of reports, it was not always clear how the risk of gender-based violence was defined, or how companies came to determine the level of risk rating assigned, including severity, probability, and likelihood.** Definitional approaches

varied: some companies provided a definition, some linked their definitions to existing guidance, some provided sub-categories of harms that fall into the category of online gender-based violence. The reports also had a varying level of detail in describing the risk.

- **Companies can further explore how design features lead to negative experiences in relation to gender-based violence, including doing further research and sharing evidence to inform design.** Civil society organisations have created "prevention by design" resources with suggestions for evidence-based design measures that could better voluntarily combat gender-based violence, including improved nudges, user controls, user onboarding and awareness, feedback mechanisms, documentation tools for victims, reporting features, etc. However, these also create the possibility of unintended impacts and need to be carefully considered in this context. For example, malicious actors can use complaints mechanisms to try to remove content on women's health. Perpetrators can use the same technologies designed as mitigations to track and monitor activity. Prevention by design mitigation measures can be a step in the right direction, but it is important to consider potential tradeoffs and impacts on rights.

B. RISKS OF TERRORIST AND VIOLENT EXTREMISM CONTENT IN RELATION TO PRODUCT DESIGN

- **"Borderline" content remains a key challenge.** This includes content that is legal but perceived as harmful (e.g., provocative, political, or controversial speech), which can be misclassified under platform counter-terrorism policies. This creates a gray area where expression is at risk of being wrongfully removed. Some companies are aiming to draw the clearest possible lines with localised policies that can be enforced at scale, with regular refinement of those policies, enforcement, and other controls like notice and appeal, but persistent challenges remain.

- **The metrics that companies and stakeholders use to assess risks of terrorist content are particularly important, as the impact of terrorist content can be very severe, even if the overall prevalence of the content is low. This points to the need to combine quantitative and qualitative metrics on impact with metrics related to scope and scale.** The mitigations need to be adjusted accordingly, to mitigate the severe risk while guarding against overly sweeping enforcement measures that can restrict lawful content and ignore contextual nuance.

- **Automated tools are key resources, but remain opaque and error-prone.** Systems like hash matching, keyword blocking, and content blocklists (including so-called "search

term isolation" lists) are widely used to detect and remove content before users report it. These tools rely predominantly on already identified content and frequently lack transparency and context, making it difficult for users to understand or challenge decisions.

- **The discriminatory impacts of overmoderation are well documented. Despite this, platforms often fail to build protections into their enforcement systems and designs, especially automated ones.** Content moderation systems disproportionately target users from Arab, Muslim, and other racialized communities. Benign phrases are sometimes mistranslated or taken out of context, reinforcing systemic bias. It's not clear if companies are investing resources in languages that are not official languages of the EU, such as Parsi, Hebrew, and Arabic. Legal carve-outs are also not consistently respected. Under EU law (Terrorist Content Online Regulation or TERREG), journalistic, academic, artistic, and research content is explicitly excluded from being treated as terrorist content, and the assessments should further emphasise how these exemptions are considered.

- **The Digital Services Act obliges platforms to conduct meaningful risk assessments and adopt proportionate mitigation measures, which means more than simply content takedowns.** For example, mitigation measures should include details on automated detection, error rates, and the nature of enforcement actions.

- **Rights-respecting moderation requires transparency, safeguards, context and a focus on the design of the product and a proportionate mitigation strategy.** Companies have different moderation models, with varying levels of thresholds for restrictions. But, these approaches are rarely explained in detail publicly, leaving users uncertain about thresholds, escalation, or appeal processes. Respecting freedom of expression and due process is essential to avoid turning counter-terrorism tools into mechanisms of censorship.

- **Company participation in multistakeholder forums can help ensure that counter-terrorism efforts do not become tools of censorship or discrimination.** Civil society organisations and human rights experts should especially be consulted in shaping mitigation frameworks.

C. DRAFT GUIDELINES ON THE PROTECTION OF MINORS ONLINE UNDER THE DIGITAL SERVICES ACT IN RELATION TO CHILD RIGHTS ASSESSMENT BEST PRACTICES

Organiser note: At the time of the event, the guidelines were in draft and the summary of the discussion reflects that. Since then, the final version has been published.

- **The European Commission's draft guidelines are a useful starting point, but there are shared areas of concern.** It is reasonable to focus on limiting access by minors to restricted content such as online pornography, gambling, and information about alcohol. It's also encouraging that the draft seems to reflect the expertise of civil society organisations, who have pointed out the risks associated with "engagement optimization" and the importance of prioritizing explicit user signals rather than or in addition to implicit platform signals. However, stakeholders identified a few shared areas of concern (see following bullets) that can be improved in the final version.

- **The draft guidelines articulate four high level principles: privacy, safety, and security by design; age appropriate design; proportionality; and children's rights. However, the guidelines do not resolve the inherent tensions between them.** For example, the guidance includes age restriction, which could result in new data collection, thereby raising privacy concerns. While there is agreement that, where platforms have relevant information, they should be considering design features that reduce risks to minors, more content and guidance would be welcome on how platforms could think through different risks and mitigations and navigate trade-offs.

- **The draft guidelines focus on implementing "age-appropriate design", including age verification. These approaches could have disproportionate impacts on access to online services,** particularly as the guidelines apply to all online platforms, not just platforms designated as Very Large Online Platforms or Search Engines (VLOP/VLOSEs), and influence freedom of expression.

- **Child rights assessment best practices encourage assessments to focus on the whole scope of "child rights"** as defined by the Convention on the Rights of Child and evaluate those rights across the whole platform for possible impacts. In particular, it is not clear that the draft guidelines engage sufficiently with children's evolving autonomy and right to seek information as they get closer to adulthood.

- **While the draft guidelines are intended to be flexible so companies with varying products can apply them, it's not clear if they are achieving that goal.** Some

provisions are highly prescriptive, raising concerns that they could conflict with the protection of fundamental rights (e.g. protecting minors from "unrealistic beauty standards"). More broadly, there were concerns that over-specificity of the types of risks and mitigations required could encourage an approach that closes rather than open discussions to a broader range of risks.

Cross-cutting recommendations

- **The European Commission should offer more guidance on defining risks, without being overly prescriptive. Regardless, companies can provide more comprehensive definitions of risks they are assessing,** along with how they determine the level of risk rating assigned, including severity, probability, and likelihood.

- **Both civil society and companies need to more holistically consider the design of mitigations in their specific risk context for the possibility of unintended impacts on rights and flattening of nuance,** as many mitigation measures present risks of their own.

- **Companies should better explain the thresholds of their moderation policies,** especially in relation to escalation and appeals, recognizing the need to guard against adversarial abuse.

- **Companies should consider using "design from the margins" approaches, so that the most impacted people inform design and everyone benefits from their insights with improved product design.** In doing so, practitioners should take care not to take a paternalistic tone or talk in overly broad strokes about marginalized and criminalized communities.

- **The European Commission's draft guidelines on the protection of minors should include more guidance on how to resolve the inherent tensions between their identified principles, and better take into account child rights assessment best practices.**

04 Use more data and metrics to show validity, effectiveness, and improvement over time.

Key learnings

- **Center the desired impact of the DSA's regulatory framework in risk assessments, evaluations, and conversations about risk.** The goal is to both protect people's rights, address harms as they emerge, and reduce future harm. We need better data to evaluate whether that is actually happening.

- **Civil society organisations are still not sure which risks are most prevalent, or what data went into determining risk levels.** Civil society experts said that while they appreciate having public versions of risk assessment methodologies, it is often hard to trace back the assessment terminology to real life impacts. In their view, the reports are sharing pieces of information about risks and harms, but still do not give an overall picture of what risks are most prevalent or problematic. This means the results of platform risk assessments are difficult for civil society to verify or contest.

- **From the company perspective, a DSA risk assessment report is limited to the scope of the law and not designed to be a line by line publication of every risk the company faces,** as that would be operationally burdensome and not practical towards achieving the overall goal of reducing harms and protecting rights; instead, they see these reports as a high level view of a broad set of risks and mitigations that are one component of their broader due diligence efforts. Sometimes companies are considering possible risks and determining they are not salient, and not including that in the assessment report. Further, the audit requirement of the DSA risk assessment means that each risk assessed must include robust accompanying evidence to support conclusions, which limits companies' ability to adopt customized approaches year over year.

- **It is critical to have more comprehensive and systematic information and data on the extent to which mitigation measures work as intended.** Otherwise the risk assessments are a "black box"; stakeholders can review the methodology and outputs, and the accompanying audit, but they don't have a way to assess the effectiveness of mitigations or access the data that underpins those determinations by companies, auditors, and/or regulators. The lack of externally-verifiable data and metrics to validate assessments also limits comparability across services and over time. Finding

ways to share more of the data is a crucial part of making risk assessments meaningful, including through DSA Article 40. This also ties into enabling continuous improvement of risk assessment and mitigation over time, and ensuring safeguards for rights-based approaches.

- **Civil society organisations would like to see more comparability across the reports, when it is possible. This would enable more of an ecosystem level understanding of risks and mitigations across platforms and services, and easier access to useful information over the long-run.** For example, comparability would be particularly useful across the types of risks assessed and a minimum set of metrics in relation to the scale and scope of risks, such as the percentage (or another systemized scale) of users affected by a risk. Frameworks like the UNGPs and the DTSP Safe Framework might be useful in enabling more comparability and suggesting possible metrics. This also ties into coherence across regulatory regimes.

Recommendations

- **Companies should share more quantitative data on risk prevalence, including on specific risks in specific regions and/or countries across Europe, and on the effectiveness of mitigations.** This would help civil society organisations compare across reports and better know where to focus their efforts, which in turn would help companies better understand and possibly reduce more prevalent risks. Quantitative data could also be accompanied by qualitative explanations.

- **Companies should consider sharing better qualitative information to help with understanding the intersections of risks across services,** the actual impact of risks, and risks across the ecosystem as a whole. For example, to understand how companies assess proportionality, it could be useful to have more qualitative information (including case studies) about alternative mitigation measures that the company considered but decided not to implement and why.

05 Address persistent tensions in meaningful stakeholder engagement.

Key learnings

- **The first round of assessment reports all discuss conducting some form of external stakeholder engagement, but the extent of it, specificity of what it covers, and approaches to engagement range quite widely.**

- **The existing asymmetries between civil society and companies in stakeholder engagement remain, and if anything, have heightened over the last year.** These include asymmetries in power, resources, technical capacity, and access to information. These disparities materialize differently, with varying levels of impacts, across civil society organisations. They have broadly resulted in a trust deficit between civil society and companies. And, on top of that, the funding and political environment has become more difficult for civil society organisations.

- **There's a window of opportunity to define this regulatory system over the next few years, so meaningful engagement now between regulators, companies and civil society is critical.** But, the many deficits in stakeholder engagement need to be addressed. Civil society organisations need to be able to show more immediate impact from their engagement with companies for their own stakeholders (including communities, members, partners, funders, etc.). If companies don't meaningfully engage civil society or aren't coordinated enough to engage them productively, the ability for civil society to focus time and energy on company engagement (in addition to other priorities such as public advocacy or engaging regulators) likely will reduce. The timing of this engagement also matters; engaging civil society during decision-making processes is more useful to both sides than after decisions are made or reports are published.

- **There is still a disconnect within companies between their broader stakeholder engagement efforts and their specific DSA engagement, and companies can do a better job of situating their DSA engagement within their overall engagement efforts.** Many companies, especially larger ones, are conducting various forms of stakeholder engagement across different functions. Some companies are trying to better internally connect the dots across their forms of engagement, so lessons are internally incorporated across functions and it's externally clearer for stakeholders

when engagement is related to the DSA. But, external stakeholders still feel there is a disconnect.

- **As noted in section 2 above, risks are different based on platform types, and so engagement with civil society will look different and evolve based on how risks show up on specific platforms.**

- **There's a lack of either understanding or communication demonstrating the impact of stakeholder engagement.** Companies could better represent the value of the stakeholder engagement that does happen, and not just on the basis of regulatory requirements, and share that back with civil society, regulators, and others.

- **Engagement needs to go beyond civil society organisations, to include impacted users, communities, and other relevant practitioners.** Sometimes global civil society organisations make recommendations for a whole community, when in reality those recommendations can create negative effects in marginalised communities. Also, digital rights civil society organisations might not always have the risk specific expertise that is needed.

Recommendations

- **The European Commission should further clarify their expectations for meaningful stakeholder engagement under Recital 90 through published guidance.** Currently, there are different expectations for what counts as meaningful engagement across companies and civil society. The European Commission could also improve their own coordination with stakeholders. Stakeholders report hearing conflicting messages from different contact points at the Commission, and without formal guidance, it is difficult to parse and rely on.

- **Companies should make clear who the point(s) of contact are for civil society to send questions and resources, and have a process to acknowledge receipt.** The lack of clear points of contact is a persistent pain point for civil society organisations, who want to send their research to inform risk assessment but often do not know how to reach the relevant people within companies.

- **Companies should acknowledge persistent asymmetries, and address them where possible,** including approaching civil society organisations and experts proactively, developing ongoing relationships with feedback loops, consulting on how to structure engagement, and committing to sharing new information so conversations don't

stall over time. This could also include funding support, with appropriate firewalls for independence of civil society.

- **Companies should be clear when ongoing stakeholder engagement might inform DSA risk assessment and mitigation,** and consider hosting specific engagements in relation to the DSA. There should be different forms of engagement, both formal structured feedback processes on regular cadences, and informal engagement as needed.

- **Companies should consider designing engagements that offer input into mitigation design, testing, and evaluation of effectiveness and proportionality.** It's especially useful for companies to share what recommendations they have already received from civil society, as some recommendations could inadvertently lead to disproportionate measures, but with enough background information stakeholders can offer more concrete and proportionate recommendations.

- **Companies should seek to broaden their networks for consultation over time and not rely on the same stakeholders for feedback.** They should also seek to consult groups other than civil society organisations and researchers, such as risk specific experts and users. Finally, they should meaningfully include non-European stakeholders, as their insights are relevant to understanding how risks can evolve and change online.

- **Civil society organisations should come to consultations prepared to share both broad feedback and specific thematic and product feedback.** Recognizing that time is a resource, and civil society is resource constrained, it is helpful if stakeholders review publicly accessible materials in advance of consultations and come with related questions and feedback.

06 Clarify the role of DSA audits and auditors with regard to risk assessment and mitigation.

Key learnings

- **Auditors are *not* confirming or validating the findings of the risk assessment, nor are they evaluating risk assessments from a human rights perspective.** For DSA audits, auditors evaluate whether the company has been operating in compliance with the law. Pursuant to Article 13 of the European Commission's *Delegated Regulation on independent audits under the Digital Services Act,* the assessment of the audited

provider's compliance with Article 34 must include but not be limited to: how the audited provider identified, analyzed, and assessed the risks that are linked to its service; what information was used; and whether they "tested assumptions on risks with groups most impacted by the specific risks." There was not a clear understanding across civil society of how auditors were carrying out this analysis, and in particular how they assessed the efforts by companies to engage such groups.

- **In cases where the European Commission is investigating whether companies have diligently assessed risks and put in place effective and proportionate mitigations, auditors have been reluctant to audit these requirements.** Few auditors examined risk assessments and mitigations under investigation by the European Commission.

- **From the company perspective, the audit adds a high level of complexity and operational burden, without necessarily generating commensurate benefit to user rights or effectiveness.** For each risk area identified, companies must get into significant detail through the audit, in addition to the risk assessment itself. This consumes significant time and resources, including from teams that actively tackle these critical risks on a day-to-day basis.

- **Given the yearly cadence of assessment and audits, and the lack of time between them, there is not enough time and opportunity for companies to comprehensively adapt their practices year-on-year** and to share learnings across internal teams and from external sources.

Recommendations

- **In the near term, the European Commission can further clarify the intended objectives of audits and assess whether audits are meeting these. In the medium to long term, the Commission and Parliament may want to consider adapting the timeline and process related to audits,** including reducing the cadence and required level of assurance, as many stakeholders shared during the draft consultation.

- **Civil society should seek to foster conversation about how to make audits most effective, rights-respecting, and efficient.** In doing so, civil society can seek to engage with auditors to build their knowledge and capacity about human rights and risks, as well as how to evaluate company efforts to engage relevant stakeholders.

07 Aim for rights-respecting coherence of risk-based online regulatory frameworks.

Key learnings

- **Company and civil society stakeholders have identified that further guidance would improve the practice of DSA risk assessments, but there is not yet a clear picture of what *kind and level* of guidance would make risk assessment effective, rights-respecting, comprehensive, coherent, and potentially comparable.** There is still room and possibility for DSA risk assessment guidance and shared methods; but it also could be challenging to introduce standards a few years into regulatory implementation, as companies have already invested in developing their processes and teams over the last few years. There was both frustration with and appreciation for the European Commission's approach of not setting out detailed risk assessment guidance and standards. There is still an ongoing challenge of understanding and comparing company approaches to risk assessment and mitigation. But, there is also a recognition of the need to guard against overly-prescriptive approaches that could create barriers for smaller platforms, new entrants, specific product types, etc.

- **In the interim, without DSA risk assessment guidance or a set of standards, platforms are looking to guidance from other regulators and stakeholders.** While this could bring more clarity to DSA assessments and begin to cohere different regulatory frameworks, it also could create unwanted intersections between regulatory frameworks and "spillover effects". In practice, the risk assessment guidance produced by Ofcom under the UK's Online Safety Act (OSA) has been a reference point for companies. Some companies also drew on the DTSP's Safe Framework to guide their approach to risk assessments, using it as a practical tool to identify, evaluate, and mitigate potential harms in line with the DSA's requirements. Regardless, it will take time for "good practice" to slowly cohere within companies and across regulatory frameworks.

- **Unclear and/or uneven interpretation of the DSA creates risks for users and companies in Europe, as well as opportunities for less rights-respecting governments to co-opt the language of the DSA in service of authoritarian impulses.** Practitioners can look to existing human-rights based frameworks like the UNGPs to inform compliance without overbroad influence from regulators.

- **Some jurisdictions outside of Europe are tying "knowledge" of specific conduct or content to platforms liability, while at the same time, risk-based frameworks (including the DSA) require these same platforms to be more transparent about conduct and content-related risks and corresponding efforts to mitigate them.** As a result, there can be a tension between these two kinds of regulatory regimes, where "identifying risks" under the DSA could increase exposure to liability under other regimes in ways that could be concerning for freedom of expression.

- **For smaller platforms, it remains a huge lift to complete risk assessments on an "at least" annual basis. This can result in a reduction in their ability to invest in voluntary safety efforts in the EU, as well as other jurisdictions.** Harmonization and coherence across international frameworks can help ensure that regulation does not create barriers to new entrants and competition, and facilitate greater civil society participation in both the conduct and evaluation of risk management. However, standardized templates for completing risk assessments would likely not be helpful, given the wide range of platforms.

- **Within Europe, practitioners should expect interaction between the DSA and a number of regulatory frameworks,** such as those set out in the AI Act, especially with the possibility of AI companies starting to be regulated under the DSA, the Digital Fairness Act, the European Media Freedom Act, the Corporate Sustainability Due Diligence Directive, and others.

- **Practitioners should be thinking about emerging technologies in the context of the many risk-based regulatory frameworks around the world.** There are tensions to navigate between ensuring specific compliance, given how different risks can be on different platforms, and making sure frameworks and standards can be adapted and are not overly overburdensome.

Recommendations

- **The European Commission or an external multistakeholder body should consider developing clearer guidance on how to conduct effective and rights-respecting DSA risk assessments** in ways that embed human rights approaches into risk assessment methodology (see more in section 1), identify synergies with other similar, democratically-enacted regulatory regimes, and avoid overly prescriptive approaches. Regardless of who develops this guidance, civil society and companies can collectively identify where, when, and how additional regulatory risk management guidance can be useful to protect rights and where it can be harmful to them.

- **The European Commission, companies, or an external multistakeholder body should develop a shared taxonomy of possible mitigations that platforms could consider.** This could be a useful tool to reduce the burden of compliance (especially for smaller platforms), increase coherence across regulatory frameworks, and embed rights-based approaches into consideration of mitigations.

- **Civil society should continue to scrutinize the implementation and enforcement of the risk assessments under the DSA to ensure respect for human rights and user safety.** As noted above, civil society needs support and resources to continue to play this vital role.

Conclusion

This was the first DTSP and GNI-hosted opportunity to discuss risk management under the DSA since the publication of DSA risk assessments, mitigations, and associated audits. Representatives from digital services and civil society brought a range of perspectives to the discussion and were able to identify gaps in risk assessment reports and stakeholder engagement practices, challenges and lessons learned from the past year of risk assessments, comparative learnings from across regulatory regimes, and points of common ground towards the goals of protecting user rights and reducing risks online. This report offers a number of recommendations for civil society, companies, and the European Commission to enable risk assessments to serve the purpose of continuous learning and encourage rights-based approaches to DSA risk assessment and mitigation. DTSP and GNI look forward to continuing these conversations in other fora and through this annual event series.

ANNEX I: Resources

These are some of the resources that the organisers used to prepare for the Forum, that participants shared 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.

- **CDT Europe & the DSA Civil Society Coordination Group:** Civil Society Responds to DSA Risk Assessment Reports: An Initial Feedback Brief
- **CELE:** Are Risks the New Rights? The Perils of Risk-based Approaches to Speech Regulation
- **De|Center:** What is Design From the Margins?
- **DSA Research Network Circle of Friends:** Recap of the 2nd Meeting
- **Dunstan Allison Hope:** Is Additionality More Important than Comparability?
- **Dunstan Allison Hope:** What Article 34 of the DSA Could Have Said
- **ECNL & Access Now:** Towards Meaningful Fundamental Rights Impact Assessments Under the DSA
- **Future of Free Speech:** Safeguarding Freedom of Expression in the AI Era | TechPolicy.Press
- **Future of Free Speech:** The DSA Enforcement Tracker
- **Future of Free Speech:** Who Decides What's Good for Society? AI, the DSA, and the Future of Expression in Europe
- **Global Disinformation Index: submissions to the European Commission** https://disinfocode.eu/reports?signatory=global-disinformation-index&type=
- **GNI:** Ensuring Digital Services Act Audits Deliver on Their Promise | TechPolicy.Press
- **Integrity Institute:** Integrity Institute Releases New Transparency Resources
- **Integrity Institute & Search for Common Ground:** New Report Calls for Proactive Solutions to Tech-Facilitated Gender-Based Violence

- **Knight Georgetown Institute:** Better Feed's EU Policy Brief
- **Knight Georgetown Institute:** From Ambiguity to Accountability: Analyzing Recommender System Audits under the DSA | TechPolicy.Press
- **Liberties & European Partnership for Democracy:** Civic Discourse and Electoral Processes in the Risk Assessment and Mitigation Measures Reports under the Digital Services Act: An Analysis
- **Liberties & European Partnership for Democracy:** Beyond Disinformation: How DSA Risk Assessments Ignore Democracy's Real Threats | TechPolicy.Press
- **Oversight Board:** Why Freedom of Expression Must Be The Centerpiece of Systemic Risk Assessments
- **UNICEF:** Child Rights and Business
- **United Nations Office of the High Commissioner for Human Rights (OHCHR):** Response to the European Commission consultation on draft act on researcher access to data under the EU Digital Services Act
- **WHAT TO FIX:** Submission to the European Board on Digital Services' Annual Report on Systemic Risks

We are also sharing a few resources on stakeholder engagement best practices:

- **BSR:** Effective Engagement with Technology Companies- A Guide for Civil Society
- **ECNL:** Framework for Meaningful Engagement
- **GNI & Global Partners Digital:** Engaging Tech Companies on Human Rights
- **OECD:** Due Diligence Guidance for Responsible Business Conduct (especially pp. 49-51 sections on Meaningful Stakeholder Engagement)
- **UN:** Guiding Principles on Business and Human Rights (UNGPs) (especially pp. 19-20, Principle 18)

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

- 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
- Centre on Regulation in Europe (CERRE)
- Knight Georgetown Institute
- Sciences Po Law School
- Swansea University
- University College London, Gender & Tech Research Lab
- University of Amsterdam, Institute for Information Law, DSA Observatory
- University of Namur

Civil Society and International Organisations

- 7amleh
- ARTICLE 19
- BSR
- Center for Democracy and Technology (CDT) Europe
- Christchurch Call

- CIPESA
- Civil Liberties Union for Europe
- De|Center
- Electronic Frontier Foundation (EFF)
- European Partnership for Democracy (EPD)
- Future of Free Speech
- GIFCT
- Global Partners Digital (GPD)
- HateAid
- Independent
- Integrity Institute
- Oversight Board
- Search for Common Ground
- Tech Coalition
- Tech Global Institute (TGI)
- TechFreedom
- The Global Disinformation Index (GDI)
- WeProtect Global Alliance
- What to Fix
- Office of the United Nations High Commissioner for Human Rights (UN OHCHR)
- UNICEF

Companies / Platforms

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

About the Organisers

Several representatives from DTSP and GNI attended the Forum, as did a representative from GNI's outside legal counsel, White & Case LLP.

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, in particular when addressing overly broad government requests and restrictions.

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

Tuesday, 3 June

11:15 AM - 12:15 PM	**Welcome & Scene-Setting**
11:15 AM - 11:30 AM	Welcome & objectives from organisers
11:30 AM - 12:15 PM	Expert plenary briefing and Q&A "What are key DSA risk assessment developments?"
12:15 PM - 1:00 PM	**Lunch**
1:00 PM - 2:45 PM	**Part 1: Considering platform type: better assessing risks and tailoring mitigation measures while protecting fundamental rights**
1:00 PM - 2:00 PM	Concurrent workshops **Objectives:** • Information sharing from companies to civil society on how different platform types are tailoring specific risk factors identified in Article 34.2 in their assessments. • Information sharing from civil society to companies on how their work/analysis might be useful in considering relevant risks on various platforms, and specific mitigation measures and their impacts on rights.

Topics and questions:

- Which risks were identified as more (or less) prevalent on different platform types in the most recent DSA risk assessments, and how do those risks manifest and present themselves? Are platforms seeing changes to risk prevalence since last year?
- How are different platform types considering the more prevalent risks given the factors identified in Article 34.2 (see below)?
    - the design of their recommender systems and any other relevant algorithmic system;
    - their content moderation systems;
    - the applicable terms and conditions and their enforcement;
    - systems for selecting and presenting advertisements;
    - data related practices of the provider.
- What specific tools do different platform types have at their disposal to mitigate these risks?

WORKSHOP 1A:
SEARCH ENGINES AND KNOWLEDGE PLATFORMS
With a cross-cutting focus on design of recommender systems and any other relevant algorithmic system.

WORKSHOP 1B:
SOCIAL MEDIA PLATFORMS
With a cross-cutting focus on content moderation systems.

WORKSHOP 1C:
APP STORES AND MARKETPLACES
With a cross-cutting focus on the data related practices of the provider.

2:00 PM - 2:30 PM	**Plenary debrief** on workshops on assessing risks in relation to platform type
2:30 PM - 2:45 PM	Coffee Break

2:45 PM - 5:15 PM	**Part 2: Better assessing risks and tailoring mitigation measures while protecting fundamental rights**
2:45 PM - 4:45 PM	Concurrent workshops

WORKSHOP 2A: ASSESSING AND MITIGATING RISKS OF GENDER-BASED VIOLENCE IN RELATION TO PRODUCT DESIGN

Objectives:

- Information sharing from companies to civil society on how gender-based violence risk assessments within companies consider product design; how companies are considering and implementing related mitigation measures; and how they are balancing possible impacts to rights as they consider mitigation measures.
- Information sharing from civil society to companies on how their work/analysis might be useful in considering risks related to gender-based violence, and specific mitigation measures and their impacts on rights.

Topics and questions:

- What relevant risks did companies identify in their assessments last year? How are they considering these risks in this year's assessment? What's changed?
- How did companies identify and consider mitigations in last year's assessment on these topics? How are they developing mitigations in relation to this year's assessment?
- How are companies determining what mitigations are reasonable, effective, and proportionate, including balancing the possible negative impacts on rights from mitigations themselves?

WORKSHOP 2B: ASSESSING AND MITIGATING RISKS OF TERRORIST AND VIOLENT EXTREMISM CONTENT IN RELATION TO PRODUCT DESIGN

Objectives:

- Information sharing from companies to civil society on how terrorist and violent extremism content risk assessments within companies consider product design; how companies are considering and implementing related mitigation measures; and how they are balancing possible impacts to rights as they consider mitigation measures.
- Information sharing from civil society to companies on how their work/analysis might be useful in considering risks related to terrorist and violent extremism content, and specific mitigation measures and their impacts on rights.

Topics and questions:

- What relevant risks did companies identify in their assessments last year? How are they considering these risks in this year's assessment? What's changed?
- How did companies identify and consider mitigations in last year's assessment on these topics? How are they developing mitigations in relation to this year's assessment?
- How are companies determining what mitigations are reasonable, effective, and proportionate, including balancing the possible negative impacts on rights from mitigations themselves?

WORKSHOP 2C: CONSIDERING DRAFT GUIDELINES ON THE PROTECTION OF MINORS ONLINE UNDER THE DIGITAL SERVICES ACT IN RELATION TO CHILD RIGHTS ASSESSMENT BEST PRACTICES

Objectives:

- Collectively better understand and share thoughts about the European Commission's draft guidelines, particularly in light of upcoming consultations.

	Topics and questions: • How do the draft guidelines build on previous risk assessments? • How will the draft guidelines change how companies approach risk assessments and mitigations around the protection of minors? • What do the draft guidelines do well and what could be improved? What is unclear? • How do the draft guidelines align with emerging best practices for assessing child right impacts?
4:45 PM - 5:15 PM	**Plenary debrief** on concurrent workshops considering product design
5:15 PM - 6:30 PM	Reception

Wednesday, 4 June

9:00 AM - 9:30 AM	**Welcome & Scene-Setting**
9:30 AM - 11:30 AM	**Part 3: Enabling deeper shared learning and more rights-based assessments**
	Objectives: • Collective brainstorming to identify existing good practices and gaps in making risk assessments more of a learning exercise and more rights-based. • Collective brainstorming to develop possible recommendations to actors across the field to make risk assessments more of a learning exercise and more rights-based.
9:30 AM - 10:00 AM	**Multistakeholder lightning remarks in plenary,** on enabling deeper shared learning and more rights-based assessments.
10:00 AM - 11:00 AM	Discussion-based workshop in small groups **Continuous learning:** • What existing good practices support continuous learning? • What are the gaps in supporting continuous learning? • Who are the relevant actors to enable continuous learning? • What recommendations might be made to those actors to enable more continuous learning? **Rights-based assessments:** • What existing good practices support rights-based approaches to risk assessment and mitigation? • What are the gaps in supporting using more rights-based approaches? • Who are the relevant actors to enable more rights-based approaches?

	• What recommendations might be made to those actors to enable more rights-based approaches? • What recommendations might be made to those actors to enable more rights-based approaches?
11:00 AM - 11:30 AM	Plenary debrief
11:30 AM - 1:00 PM	**Lunch and open time for follow up questions and connections**
1:00 PM - 2:30 PM	**Part 4: What's next: imagining a rights-respecting future together?**
1:00 PM - 2:00 PM	Panel & Q&A **Topics and questions:** • What did we learn over the last two days? • What outcomes should practitioners be driving towards within the DSA risk assessment regulatory framework? • Where do we go from here to ensure that DSA risk assessments mitigate risks while protecting fundamental rights?
2:00 PM - 2:30 PM	Concluding remarks from the organisers

GLOBAL NETWORK INITIATIVE

Digital Trust & Safety Partnership