weizenbaum journal OF THE DIGITAL SOCIETY

J\05 ISSUE 02

WEIZENBAUM JOURNAL OF THE DIGITAL SOCIETY
Volume 5 \ Issue 2 \ w5.2.6 \ 06-16-2025
ISSN 2748-5625 \ DOI 10.34669/WI.WJDS/5.2.6

Information on this journal and its funding can be found on its website:
https://wjds.weizenbaum-institut.de

KEYWORDS

platform governance
platform regulation
digital services act
risk management
risk regulation

RESEARCH PAPER

The Politics of Risk in the Digital Services Act

A Stakeholder Mapping and Research Agenda

Rachel Griffin

Sciences Po Law School
rachel.griffin@sciencespo.fr

ABSTRACT

The EU's 2022 Digital Services Act requires large online platforms to regularly assess and mitigate 'systemic risks' to various public-interest goals, including fundamental rights, civic discourse, public health and security. Drawing on social constructionist understandings of risk, this article theorizes systemic risk management under the DSA as an arena for political power and contestation, since translating its broadly-defined abstract principles into actionable risk management procedures will entail making many contestable political decisions about how online platforms should be governed. This raises the question: *who* will exercise power in these decision-making processes? Providing some first answers to this question, this article makes three key contributions. First, it maps the key stakeholder groups involved, and the legal and institutional mechanisms through which they can participate in DSA systemic risk management. Second, it critically analyzes the power dynamics and unequal resources that will structure stakeholder participation. Third, this stakeholder mapping provides a foundation for future research on the politics of DSA systemic risks. The article concludes with reflections on directions for future research on the political agendas, priorities and strategies that shape platform governance.

1 Introduction

Articles 34–35 of the EU's 2022 Digital Services Act require the largest online platforms (those with over 45 million EU users[1]) to regularly assess and mitigate 'systemic risks' related to various broadly-defined public-interest goals and concerns: dissemination of illegal content; fundamental rights; public security, electoral integrity and 'civic discourse'; and public health, people's physical and mental wellbeing, and minor safety. This long list of broad and ambiguous topics could encompass a huge range of policy issues related to platform governance. However, there is a strong consensus that disinformation is one of the key systemic risks – as reflected, for example, in the European Commission's first official guidelines on risk mitigation (which dealt with Russian disinformation operations,[2] and with electoral interference more generally[3]). The 2022 Code of Practice on Disinformation (an updated version of a non-binding code developed in 2016) became the first official DSA code of conduct in February 2025,[4] which means it now provides authoritative guidance on risk mitigation.[5]

This is not an immediately obvious interpretation of Articles 34–35, which do not explicitly mention disinformation. Disinformation campaigns, coordinated manipulation, and fake or bot accounts are mentioned in Recitals 83–84, 88 and 104, as examples of the types of issues platform companies should consider in relation to electoral integrity, civic discourse, and public health and security, but these are only examples, representing some of the many possible understandings of these risk areas. The consensus that disinformation is a key systemic risk does not result from a literal or self-evident application of the legislative text. Rather, this understanding of risk has been actively produced, through years of research and discussion in expert communities spanning pol-

---

1 See Art 33 DSA, Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance) [2022] OJ L227/1 ('DSA'). 'Online platform' in the DSA means a service that hosts user-generated content and disseminates it to the public (see Art 3(i)).

2 European Commission, 'Digital Services Act study: Risk management framework for online disinformation campaigns' (30 August 2023) https://digital-strategy.ec.europa.eu/en/library/digital-services-act-study-risk-management-framework-online-disinformation-campaigns accessed 21 January 2025.

3 European Commission, 'Guidelines for providers of VLOPs and VLOSEs on the mitigation of systemic risks for electoral processes' (26 April 2024) https://digital-strategy.ec.europa.eu/en/library/guidelines-providers-vlops-and-vloses-mitigation-systemic-risks-electoral-processes accessed 21 January 2025.

4 European Commission, 'The Code of Conduct on Disinformation' (13 February 2025) https://digital-strategy.ec.europa.eu/en/library/code-conduct-disinformation accessed 31 March 2025.

5 Article 45 provides that codes of conduct can be developed 'to contribute to the proper application of this Regulation, taking into account in particular the specific challenges of tackling different types of illegal content and systemic risks': see Art 45(1), DSA (n 1). For a more detailed analysis of the legal status of such codes, see Rachel Griffin, 'Codes of Conduct in the Digital Services Act: Functions, Benefits & Concerns' (2024) Technology & Regulation 167 https://doi.org/10.26116/techreg.2024.016.

itics, media, academia and civil society, in Europe and elsewhere (an institutional ecosystem that Joseph Bernstein jokingly terms 'Big Disinfo'[6]).

Yet beneath this surface consensus, we find ongoing scientific disagreement and uncertainty around basic questions such as the prevalence of online mis- and disinformation; how (if at all) they impact political views or behavior; and what (if anything) risk mitigation measures such as fact-checking achieve.[7] Some commentators argue that constructing political disagreement and instability in terms of people being 'misinformed' conveniently allows politicians, news publishers and other elite actors to avoid confronting deeper conflicts and structural problems.[8] Others believe disinformation operations pose serious risks, but point out that their success in stoking divisions and mistrust largely depends on public reactions, so political and media elites drawing attention to these risks may actually be exacerbating them.[9] This argument echoes social science research on the 'social amplification of risk', which argues that the impacts of risks largely depend on how individuals and institutions communicate about and respond to them, as this leads to indirect effects that attenuate or amplify the original risk, or create new ones.[10]

There are also very different interpretations of what platform companies should do about disinformation-related risks. This has already led to high-profile conflicts around DSA enforcement. For example, public interventions by then-Inter-

---

6 Joseph Bernstein, 'Bad News' (*Harpers*, September 2021) https://harpers.org/archive/2021/09/bad-news-selling-the-story-of-disinformation/ accessed 21 January 2025.

7 Sacha Altay, Manon Berriche and Alberto Acerbi, 'Misinformation on Misinformation: Conceptual and Methodological Challenges' (2023) 9(1) Social Media + Society https://doi.org/10.1177/20563051221150412; Ceren Budak and others, 'Misunderstanding the Harms of Online Misinformation' (2024) 630 Nature 45 https://doi.org/10.1038/s41586-024-07417-w; Ullrich KH Ecker and others, 'Why Misinformation Must Not Be Ignored' (2024) American Psychologist https://doi.org/10.1037/amp0001448; Elena Broda & Jasper Strömbäck, 'Misinformation, Disinformation, and Fake News: Lessons from an Interdisciplinary, Systematic Literature Review' (2024) 48 Annals of the International Communication Association 139 https://doi.org/10.1080/23808985.2024.2323736.

8 Holly Jean Buck, 'Obsessing Over Climate Disinformation Is a Wrong Turn' (Jacobin, 24 August 2024) https://jacobin.com/2024/08/climate-disinformation-green-transition-workers accessed 21 January 2025.

9 Olga Belogolova and others, 'Don't Hype the Disinformation Threat' (Foreign Affairs, 3 May 2024) www.foreignaffairs.com/russian-federation/dont-hype-disinformation-threat accessed 21 January 2025.

10 Roger E Kasperson and others, 'The Social Amplification of Risk: A Conceptual Framework' (1988) 8 Risk Analysis 177 https://doi.org/10.1111/j.1539-6924.1988.tb01168.x.

nal Market Commissioner Thierry Breton at the outset of the Gaza genocide,[11] encouraging leading platforms to remove more disinformation and Hamas-related content, were sharply criticized by civil society organizations (and, reportedly, internal Commission staff) concerned that Breton was encouraging platform companies to suppress content deemed politically objectionable.[12]

Overall, then, the example of disinformation illustrates that what constitutes a 'risk' under Article 34 and how given 'risks' should be understood and addressed is highly contestable. This is a feature of risk regulation in general: the concept of risk is inherently ambiguous and value-laden.[13] First, there is no objective or value-free way of understanding what concepts like 'fundamental rights', 'public security' and 'civic discourse' mean, or of conceptualizing and measuring how platforms affect them. Second, risk assessment is not about knowledge for its own sake, but about understanding threats (and opportunities) in order to make decisions.[14] Risks can only be defined, assessed and managed in light of particular interests or objectives that would be harmed if the risk materialized.[15] Consequently, translating broad concepts like those in Article 34

---

11 In January 2024, the International Court of Justice (ICJ) ruled that the Israeli military's assault on Gaza amounted to a plausible case of genocide, and ordered the Israeli government to take several specific measures to comply with its obligations under the Genocide Convention, such as taking steps to prevent genocidal acts and allowing humanitarian aid to enter Gaza: United Nations Office of the High Commissioner for Human Rights, 'Gaza: ICJ ruling offers hope for protection of civilians enduring apocalyptic conditions, say UN experts' (United Nations, 31 January 2024) https://www.ohchr.org/en/press-releases/2024/01/gaza-icj-ruling-offers-hope-protection-civilians-enduring-apocalyptic accessed 6 May 2025. Since then, the Israeli government has not complied with these orders: Basema Al-Alami, 'Israel isn't complying with the International Court of Justice ruling – what happens next?' (The Conversation, 6 February 2024) https://theconversation.com/israel-isnt-complying-with-the-international-court-of-justice-ruling-what-happens-next-222350 accessed 6 May 2025. The categorization of the war on Gaza as a genocide is also supported by a detailed legal analysis published in March 2024 by the UN special rapporteur for the occupied Palestinian territories (Francesca Albanese, *Anatomy of a Genocide* (UN Human Rights Council Fifty-Fifth Session, Agenda Item 7, 25 March 2024) https://www.ohchr.org/sites/default/files/documents/hrbodies/hrcouncil/sessions-regular/session55/advance-versions/a-hrc-55-73-auv.pdf accessed 14 May 2024) and by a growing consensus among international law and genocide scholars (see, eg, Nimer Sultany, 'A Threshold Crossed: On Genocidal Intent and the Duty to Prevent Genocide in Palestine' (2024) Journal of Genocide Research https://doi.org/10.1080/14623528.2024.2351261).

12 DSA Decoded, 'Takeaways From the Webinar "Delimiting Systemic Risks in the DSA"' (DSA Decoded, 2024) www.dsadecoded.com/webinar-summary accessed 23 October 2024. This is already a well-documented phenomenon in relation to content about the Gaza genocide and advocacy for the rights of Palestinians: see Sam Biddle, 'Facebook Report Concludes Company Censorship Violated Palestinian Human Rights' (The Intercept, 22 September 2022) https://theintercept.com/2022/09/21/facebook-censorship-palestine-israel-algorithm accessed 27 April 2023; Houda Elmimouni and others, 'Shielding or Silencing?: An Investigation into Content Moderation during the Sheikh Jarrah Crisis' (2024) 8 Proceedings of the ACM Conference on Human-Computer Interaction 6 https://doi.org/10.1145/3633071; 7amleh, Palestinian Digital Rights, Genocide and Big Tech Accountability (September 2024) https://7amleh.org/storage/genocide/English%20new%20(1).pdf accessed 7 October 2024.

13 Rachel Griffin, 'Governing Platforms Through Corporate Risk Management: The Politics of Systemic Risk in the Digital Services Act' (2025) *European Law Open* https://doi.org/10.1017/elo.2025.17

14 François Ewald, 'Insurance and Risk' in Graham Burchell, Colin Gordon and Peter Miller (eds), *The Foucault Effect: Studies in Governmentality* (University of Chicago Press 1991); Mitchell Dean, 'Risk, Calculable and Incalculable' (1998) 49 Soziale Welt 25.

15 This is not just an academic analysis, but describes mainstream understandings of risk and its management in the business and policy worlds – encapsulated by the International Standardization Organization's 2018 standard on risk management, which defines risk as the impact of uncertainty on an organization's objectives: ISO, *ISO 31000: Risk Management* (2018) www.iso.org/iso-31000-risk-management.html accessed 29 October 2024.

into actionable risk management decisions necessarily involves making normative choices about how platforms should be governed. This article thus takes as its central research question: *who will participate in deciding what is a systemic risk under the DSA, and deciding how these risks will be managed?*

Existing literature on risk regulation has explored how perceptions of risk and decisions about how to manage them are shaped by a variety of stakeholders. This includes both top-down processes in which political, business and media elites advocate for their preferred problem framings and priorities, as well as more bottom-up processes, in which the daily work of professionals such as academics, consultants or data scientists produces knowledge about risks on which other political actors rely.[16] These processes create space for the exercise of political power through 'agenda-setting': the ability to influence the allocation of resources and the behavior of other actors by determining which issues are discussed and prioritized, but also how these issues are framed and interpreted, and which issues are not considered at all.[17] In Josephine Adekola's theory of risk communication, the relative power and expertise of different interest groups are key factors determining their ability to get their preferred understandings of risk onto institutional agendas, achieve consensus behind these understandings, and shape risk management in line with their own interests and ideologies.[18]

Based on this understanding of risk management as an arena for political power and contestation, this article makes three key contributions. First, it maps the key stakeholder groups and the legal and institutional mechanisms through which they can participate in DSA systemic risk management. This overview synthesizes insights from legal scholarship on the DSA; from political science and media and communications scholarship on stakeholders in platform governance; and from critical political science and regulatory studies literature on the politics of risk regulation more generally. It is also based on personal familiarity with the expert community working on the DSA and its implementation; for example, from attending conferences and specialist events,[19] as well as conversations with relevant academic, industry and civil society experts. Second, guided by Adekola's theorization of power and expertise in risk communication, the article critically analyzes the power dynamics and unequal resources that will structure stakeholder participation, pointing to how systemic risk management may favor certain perspectives and interests over others. Finally, through this stakeholder mapping – necessarily only a preliminary

---

16 Didier Bigo, 'Security and Immigration: Toward a Critique of the Governmentality of Unease' (2002) 27 Alternatives 63; Louise Amoore, *The Politics of Possibility: Risk and Security Beyond Probability* (Duke University Press 2013); Josephine Adekola, *Power and Risk in Policymaking: Understanding Public Health Debates* (Springer Nature 2022).

17 Thomas A Birkland, 'Agenda Setting in Public Policy' in Frank Fischer, Gerald J Miller and Mara S Sidney (eds), *Handbook of Public Policy Analysis* (CRC Press 2007).

18 Adekola (n 16).

19 Academic conferences in this field tend to have a strong presence of regulatory agency staff and industry experts.

overview, since DSA implementation is still in its early stages – it provides a foundation for future research on the politics of DSA systemic risks. Such research could develop a better understanding of different stakeholders' political agendas, priorities and strategies, and suggest which agendas are ultimately shaping platform governance.

Section 2 lays the conceptual foundations for this analysis by summarizing the relevant DSA provisions and developing the article's theoretical framework. It explains how risks are socially constructed through political institutions and expert communities, in ways that tend to reflect existing disparities of power and resources, but which can also be contested from both within and outside these elite communities. Section 3 then maps the key stakeholder groups in the DSA systemic risk framework. It divides these into three broad categories – regulated companies, state institutions and other external stakeholders – and identifies relevant subgroups and internal differences within each category, as well as critically reflecting on the power disparities within and between groups. Section 4 concludes the article by reflecting on possible directions for future research on the political agendas and relative power and expertise of different groups, as well as the interactions and relationships between them.

2 The Politics of DSA Systemic Risks

2.1 The DSA's Risk Management Regime

The DSA's complex risk management framework can be helpfully conceptualized as a regulatory regime. This term serves as a form of shorthand for the set of institutions, rules, practices and ideas associated with the regulation of a particular issue.[20] This enables a discussion of how different elements in such a system work together – more or less coherently – to achieve particular goals, while also recognizing differences, tensions or conflicts.[21]

Regulated companies – 'very large online platforms' or VLOPs, with over 45 million monthly active EU users[22] – have primary responsibility for assessing

[20] Christopher Hood, Henry Rothstein and Robert Baldwin, *The Government of Risk: Understanding Risk Regulation Regimes* (OUP 2001).

[21] For Hood, Rothstein and Baldwin (n 20), the concept of a regime also offers flexibility, and can mediate between micro- and macro-level analyses of regulation. Since the risks being regulated can be defined at very different levels of abstraction, the concept of a regime can be used to analyze the different actors involved in regulating relatively specific issues (eg disinformation), or to zoom out and look at a broader system (eg online platforms generally).

[22] The DSA has a tiered structure in which most obligations apply to all online platforms or content hosting services, with some exceptions for micro or small enterprises; however, Chapter III Section 5 sets out more extensive obligations – most notably the systemic risk framework – that apply exclusively to VLOPs, as defined in Art 33, DSA (n 1).

the risks associated with the functioning and use of their services in each of the risk areas listed in Article 34(1): dissemination of illegal content; negative impacts on fundamental rights; negative impacts on civic discourse, electoral integrity and public security; and negative impacts related to gender-based violence, public health, minor protection, and people's physical and mental wellbeing. Article 35 requires VLOPs to implement 'appropriate, proportionate and effective' measures to mitigate the identified risks. Overall, these articles are framed in extremely broad, ambiguous and abstract terms. VLOPs therefore have extensive discretion over how to define relevant risks and appropriate mitigation measures.

However, VLOPs are at the center of a complex regulatory regime that involves diverse actors, processes and regulatory tools. Under Article 37, risk assessments and mitigation measures must be subjected to yearly independent audits, and their compliance with Articles 34–35 is ultimately overseen by the European Commission. While the Commission has exclusive competence to enforce the relevant provisions,[23] it receives input from the European Board for Digital Services (EBDS), which represents the member state regulators responsible for DSA enforcement.[24] The EBDS can not only advise the Commission, but also publish its own guidelines on the interpretation of Articles 34–35.[25] Articles 45–47 also provide for the creation of codes of conduct to set out more detailed compliance standards and best practices. These should be drafted by VLOPs in cooperation with various other stakeholders, including private companies (eg advertisers and software providers) and NGOs, with supervision and input from the Commission and the EDBS.[26] Finally, Recital 90 provides that risk management processes should consider relevant scientific research, as well as involving consultation with affected stakeholder groups. There are also numerous provisions – notably including Article 40, which creates mechanisms for independent researchers to access data from VLOPs – that aim to facilitate independent research into systemic risks, as well as into VLOPs' compliance practices and regulators' enforcement strategies.[27]

---

23 Art 56(2), DSA (n 1).

24 Arts 61–63, DSA (n 1).

25 See Art 35(2), DSA (n 1).

26 For a detailed analysis, see Griffin, 'Codes of Conduct' (n 5).

27 For a detailed analysis, see Paddy Leerssen, 'Outside the Black Box: From Algorithmic Transparency to Platform Observability in the Digital Services Act' (2024) 4(2) Weizenbaum Journal of the Digital Society https://doi.org/10.34669/wi.wjds/4.2.3.

2.2 Power and Expertise in the Construction of Risks

From this brief overview,[28] it is already apparent that while the DSA delegates significant discretion to VLOPs, it does not give them *carte blanche*, but aims to establish an ecosystem of government, corporate and civil society stakeholders who will all have input into what issues constitute systemic risks and how VLOPs should manage them.[29] This aligns with scholarship on risk regulation, which argues that open-ended or ambiguous regulatory provisions like Articles 34-35 can be resolved as common understandings of risk coalesce within the 'interpretative communities' involved in implementing a given regulatory regime.[30] This is easier 'within sector-specific regulatory regimes where the regulated sector forms a relatively tight-knit community'.[31] Such a community is already very visible around the DSA. Conferences, events and consultations regularly bring together regulatory agency staff, academic researchers, NGOs and industry experts, providing opportunities for them to repeatedly meet, exchange information and form professional and social connections.

Importantly, however, access to and participation in this ecosystem is far from equal: as always, 'some people have a greater capacity to define risk than others'.[32] Scholarship on the social amplification of risk argues that interest group politics is a crucial factor shaping how people and institutions understand risks. Stakeholder groups produce, mobilize and frame evidence in order to shape risk management in ways that favor their own ideologies or interests, and that help marshal support for their broader political agendas.[33] These processes are structured by pervasive disparities of power and expertise.

---

28 For a more comprehensive account of the DSA's risk management system, see Martin Husovec, *Principles of the Digital Services Act* (OUP 2024); Mateus Correia de Carvalho, 'It will be what we want it to be: Sociotechnical and Contested Systemic Risk at the Core of the EU's Regulation of Platforms' AI Systems' (2025) 16(1) JIPITEC 35.

29 Carvalho (n 28).

30 Julia Black, 'Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes' (2008) 2 Regulation & Governance 137 https://doi.org/10.1111/j.1748-5991.2008.00034.x.

31 Karen Yeung and Lee A Bygrave, 'Demystifying the Modernized European Data Protection Regime: Cross-Disciplinary Insights from Legal and Regulatory Governance Scholarship' (2022) 16 Regulation & Governance 137, 140 https://doi.org/10.1111/rego.12401. See also Hood and others (n 20).

32 Ulrich Beck, 'Living in the World Risk Society' (2006) 35 Economy & Society 329, 333 https://doi.org/10.1080/03085140600844902.

33 Adekola (n 16); Josephine Adekola, Denis Fischbacher-Smith and Moira Fischbacher-Smith, 'Light Me Up: Power and Expertise in Risk Communication and Policy-Making in the e-Cigarette Health Debates' (2019) 22 Journal of Risk Research 1294 https://doi.org/10.1080/13669877.2018.1473463; Bonnie Ram and Thomas Webler, 'Social Amplification of Risks and the Clean Energy Transformation: Elaborating on the Four Attributes of Information' (2022) 42 Risk Analysis 1423 https://doi.org/10.1111/risa.13902. Stakeholders might have a direct interest in how risk regulations are implemented (for example, regulated companies will typically favor understandings of risk that do not require them to make costly overhauls to their business practices). However, in some cases they might have an interest in shaping other actors' perceptions of risk for other reasons, for example as a way of marketing services related to risk management (consultancy, software, etc.). See Anke Sophia Obendiek and Timo Seidl, 'The (False) Promise of Solutionism: Ideational Business Power and the Construction of Epistemic Authority in Digital Security Governance' 30 Journal of European Public Policy 1305 https://doi.org/10.1080/13501763.2023.2172060.

Interest groups who have more resources, relationships with other influential actors, and capacities to produce and engage with expert knowledge will be in a better position to build consensus behind their preferred risk framings. Consequently, risks are often defined and managed in ways that stabilize existing distributions of power and resources.[34]

These points have been repeatedly highlighted in scholarship on risk regulation in general, and on multistakeholder governance structures like those created in the DSA. Civil society organizations (CSOs) generally overrepresent elite and professional classes, and different stakeholder groups have vastly different resources available for advocacy and activism.[35] Powerful industry actors like VLOPs can skew the playing field further by preferentially funding or granting access to CSOs whose perspectives are more compatible with their own interests.[36] Finally, corporate risk management obligations like those in the DSA do not only delegate significant interpretative discretion to regulated corporations, but make other actors dependent on data and information produced by these corporations. This creates further possibilities for corporations to shape the understanding of risks in ways that suit their own interests.[37]

Finally, the underlying choice to frame policy issues in platform governance as 'risks' to be managed is one that already comes with political implications, empowering certain groups over others.[38] Critical scholarship argues that risk regulation tends to favor regulated industries and established powerful interests – in particular, because it depoliticizes policy issues, framing them in terms of technical problems to be solved through professional expertise rather than more fundamental conflicts of values or interests, and pointing to incremental mitigation measures over structural reforms.[39] For instance, returning to the example of disinformation, framing public mistrust in political and

---

34 Julie Cohen, *Between Truth and Power: The Legal Foundations of Informational Capitalism* (OUP 2019).

35 Caroline W Lee, Michael McQuarrie and Edward T Walker (eds), *Democratizing Inequalities: Dilemmas of the New Public Participation* (NYU Press 2015); Rachel Griffin, 'Public and Private Power in Social Media Governance: Multistakeholderism, the Rule of Law and Democratic Accountability' (2023) 14 Transnational Legal Theory 46 https://doi.org/10.1080/20414005.2023.2203538.

36 Brenda Dvoskin, 'Representation Without Elections: Civil Society Participation as a Remedy for the Democratic Deficits of Online Speech Governance' (2022) 67 Villanova Law Review 447.

37 Julie Cohen and Ari Ezra Waldman, 'Introduction: Framing Regulatory Managerialism as an Object of Study and Strategic Displacement' (2023) 86(3) Law & Contemporary Problems i; William Boyd, 'De-Risking Environmental Law' (2024) 48 Harvard Environmental Law Review 153.

38 Griffin, 'Governing Platforms' (n 13); Rachel Griffin, 'What Do We Talk About When We Talk About Risk? Risk Politics in the EU's Digital Services Act´ (*DSA Observatory*, 31 July 2024) https://dsa-observatory.eu/2024/07/31/what-do-we-talk-about-when-we-talk-about-risk-risk-politics-in-the-eus-digital-services-act/ accessed 22 January 2025; Riccardo Fornasari and Rachel Griffin, 'Le risque est-il neutre ? Analyse comparée du devoir de vigilance et du règlement sur les services numériques' (2025) 7 Revue de droit international d'Assas 69.

39 Brian Wynne, 'Risk and Environment as Legitimatory Discourses of Technology: Reflexivity Inside Out?' (2002) 50 Current Sociology 459, 461 https://doi.org/10.1177/0011392102050003010>; Jathan Sadowski, 'Rediscovering a Risky Ideology: Technocracy and Its Effects on Technology Governance' (2020) 7(sup1) Journal of Responsible Innovation 112 <https://doi.org/10.1080/23299460.2020.1816345.

media elites as a risk caused by disruptive technologies, requiring management by an expert community which can research the problem and identify appropriate mitigation measures, could be understood as a way of deflecting more troubling questions about why people mistrust political institutions, and whether this mistrust is justified.[40]

These points appear particularly relevant to the DSA, which centrally relies on a specialized ecosystem of professional experts – auditors, consultants, academic researchers and CSOs – to produce knowledge about risks and develop best practices for risk management. This ecosystem not only favors technocratic expertise and credentials, but generally seems to assume a consensual, collaborative approach to regulatory enforcement, in which the goals are agreed upon, and the task is simply to develop technical solutions. For example, both the legal text itself and the surrounding policy discussions often frame academic researchers and civil society stakeholders as assisting regulators' and VLOPs' enforcement and compliance efforts by providing 'evidence' about systemic risks[41] – eliding the possibility that state institutions, platform companies and other actors might have fundamentally conflicting interests and ideologies.[42] This dynamic could bias DSA enforcement in a relatively conservative direction, favoring risk framings which are presented in depoliticized terms and can thus attract widespread support – including from VLOPs themselves – over those which more fundamentally challenge current approaches to platform governance.[43]

2.3 Risk Politics and Contestation

Nonetheless, these effects cannot close down contestation entirely. Because of the fundamentally ambiguous nature of risk, risk regulation is always open to different interpretations, and its implementation will ultimately be shaped by competing agendas both within and outside the expert communities involved in a given regulatory regime.[44] First, even within relatively cohesive professional communities, there will be some 'interpretative contests' over how risks should be defined and prioritized.[45] Such intra-elite conflicts have been very

40 Buck (n 8); Jeanette Hofmann, Leonie Dorn and Mikiya Heize, 'Desinformation: nicht Unkenntnis, sondern politische Verortung' (*Weizenbaum Institute*, 2024) www.weizenbaum-institut.de/news/detail/desinformation-nicht-unkenntnis-sondern-politische-verortung/ accessed 22 January 2025.

41 Leerssen, 'Black Box' (n 27); Griffin, 'What Do We Talk About' (n 38).

42 See Caroline W Lee, Kelly McNulty and Sarah Shapper, 'Civic-izing Markets: Selling Social Profits in Public Deliberation' in Caroline W Lee, Michael McQuarrie and Edward T Walker (eds), Democratizing Inequalities: Dilemmas of the New Public Participation (NYU Press 2015).

43 Griffin, 'Governing platforms' (n 13).

44 Claire Parfitt and Gareth Bryant, 'Risk Politics' (*Phenomenal World*, 7 June 2023) www.phenomenalworld.org/analysis/risk-politics/ accessed 23 October 2024.

45 Obendiek and Seidl (n 33), 1306. See also Bigo (n 16).

visible in policy debates around disinformation risks: for example, as discussed in the Introduction, the Commission's perceived overreach in encouraging platforms to suppress content related to Palestine met with significant criticism from digital rights NGOs and academics.[46] Second, even where risk framings enjoy relative consensus within expert communities, they can still be contested from outside by activists, social movements or other stakeholder groups.[47] Thomas Birkland discusses various tactics that outsider groups can use to contest regulatory institutions' agendas and problem framings – for example, allying with more sympathetic elite actors, or shifting conflicts to other venues, such as courts or media debates.[48] As section 3.3 will discuss, these tactics could be very relevant to the DSA.

Importantly, such contestation – or the mere possibility thereof – can influence how more powerful stakeholders approach risk management. Anticipating and responding to external criticism is central to what Michael Power calls 'secondary risk management'.[49] This concept describes how organizations focus not only on the 'primary' risks that they are nominally responsible for managing, but also on the 'secondary' risks to themselves if other actors should deem their risk management processes inadequate. For example, 'questions about whether businesses should employ children become questions about whether that business is public-facing and vulnerable to brand damage that could be associated with revelations of child labor in the supply chain'.[50] In the DSA systemic risk framework, the (anticipated) capacities of other stakeholders to contest risk management decisions will be an important factor shaping how VLOPs and regulators approach risk management in the first place.

A central tenet of the 'new governance' or 'decentered regulation' traditions in which the DSA can be located is making corporations more responsive to these kinds of external pressures from civil society, consumers and the public.[51] One way of understanding the DSA's risk management provisions would be to see them as a means of enabling external stakeholders to translate their understandings of 'primary' risks to the public (for example, a risk that moderation systems disproportionately censor certain perspectives) into 'secondary' risks to VLOPs' business interests (a risk of being fined for inadequately managing risks to free-

46 Daphne Keller, 'The Rise of the Compliant Speech Platform' (*Lawfare*, 16 October 2024) www.lawfaremedia.org/article/the-rise-of-the-compliant-speech-platform accessed 23 October 2024.

47 Parfitt and Bryant (n 44).

48 Birkland (n 17).

49 Michael Power, 'The Risk Management of Nothing' (2009) 34 Accounting, Organizations and Society 849 https://doi.org/10.1016/j.aos.2009.06.001.

50 Claire Parfitt, 'ESG Integration Treats Ethics as Risk, but Whose Ethics and Whose Risk? Responsible Investment in the Context of Precarity and Risk-Shifting' (2020) 46 Critical Sociology 573 https://doi.org/10.1177/0896920519868794.

51 Kenneth A Bamberger and Deirdre Mulligan, 'New Governance, Chief Privacy Officers, and the Corporate Management of Information Privacy in the United States' (2011) 33 Law & Policy 477 https://doi.org/10.1111/j.1467-9930.2011.00351.x; Julia Black and Andrew Douglas Murray, 'Regulating AI and Machine Learning: Setting the Regulatory Agenda' (2019) 10(3) European Journal of Law & Technology.

dom of expression and non-discrimination). Similarly, provisions on transparency, consultation and data access can be understood as creating institutionalized channels for external contestation of risk management decisions.[52]

Yet as section 2.2 argued, these construction and contestation processes will play out in a highly unequal landscape (a longstanding criticism of 'new governance' approaches[53]). Analyzing the politics of DSA systemic risks requires us to simultaneously appreciate the potential for contestation, but also the limits on this potential, and the structural advantages that favor constructions of risk which go with the grain of powerful state and corporate interests.

3 Mapping Stakeholder Participation in Systemic Risk Management

Building on the above analysis, this section identifies the key actors and groups who can participate in the social construction of systemic risks. This categorization draws conceptually on prior work in law,[54] political science,[55] and media studies[56] mapping stakeholder participation in platform governance.[57] Much of this work draws on the 'triangle' model proposed by Abbott and Snidal,[58] which schematically represents governance regimes in terms of interactions between states, companies and civil society.[59] Building on this model, Robert Gorwa has proposed the most detailed typology, subdividing these three overarching categories into four levels: supra-organizational,

---

52 Carvalho (n 28).

53 Ioannis Kampourakis, 'The Postmodern Legal Ordering of the Economy' (2021) 28(1) Indiana Journal of Global Legal Studies 101.

54 Dvoskin (n 36); Kate Klonick, 'The New Governors: The People, Rules and Processes Governing Online Speech' (2018) 131 Harvard Law Review 1598.

55 Robert Gorwa, 'Stakeholders' (2022) 24 Yale Journal of Law & Technology 493; Robert Gorwa, *The Politics of Platform Regulation: How Governments Shape Online Content Moderation* (OUP 2024).

56 Charilaos Papaevangelou, 'The Existential Stakes of Platform Governance: A Critical Literature Review' (2021) 31(1) Open Res Europe https://doi.org/10.12688/openreseurope.13358.2; Robyn Caplan, 'Networked Governance' (2022) 24 Yale Journal of Law & Technology 541

57 Some of this literature analyzes how interest groups influence state regulatory initiatives: see, eg, Terry Flew and others, 'Return of the Regulatory State: A Stakeholder Analysis of Australia's Digital Platforms Inquiry and Online News Policy' (2021) 37(2) The Information Society 128 https://doi.org/10.1080/01972243.2020.1870597. However, much of it focuses on how external stakeholders shape platform companies' business decisions. This latter aspect is more relevant to the construction of DSA systemic risks, as VLOPs have direct responsibility for managing risks, and other actors will thus ultimately be seeking to influence their decisions.

58 Kenneth W Abbott and Duncan Snidal, 'The Governance Triangle: Regulatory Standards Institutions and the Shadow of the State' (2009) in Walter Mattli and Ngaire Woods (eds), *The Politics of Global Regulation* (Princeton University Press 2009).

59 Papaevangelou (n 56); Robert Gorwa, 'The Platform Governance Triangle: Conceptualizing the Informal Regulation of Online Content' (2019) 8(2) Internet Policy Review https://doi.org/10.14763/2019.2.1407. See also Jack Balkin, 'Free Speech is a Triangle' (2012) 118 Columbia Law Review 2012.

organizational, sub-organizational and individual.[60] This approach facilitates analysis of disagreements and power dynamics within an organization[61] – for example, between the employees and management of a company.

Table 1: Platform governance stakeholders[62]

SUPRA	› Industry Associations	› Political Networks › Multilaterals › International Organizations	› Transnational Advocacy Networks
ORGANIZATIONAL	**Firms**	**Governments**	**NGOs**
SUB	› C-Suite › Policy Teams › Corporate Boards › Unions	› Executive Branch › Ministries › Regulatory Agencies › Intelligence Services › Police Agencies › Parliaments › Courts	› Boards of Trustees › Legal Teams › Policy + Research Teams
INDIVIDUAL	› Executives › Moderators › Employees	› Legislators › Regulators › Staffers › Judges	› Activists › Academics › Journalists › Community Mods › Ordinary Users

Building on this work, the remainder of this section identifies key stakeholder groups within each of the three overarching categories, drawing particular attention to any internal differences and conflicts, as well as disparities of power, expertise and resources within and between groups. In keeping with this article's aim of mapping the broad overall stakeholder landscape, the discussion focuses on the organizational and sub-organizational levels – although further work could analyze each of the groups discussed at even more granular levels, down to the policy agendas of individuals.

60 Gorwa, 'Stakeholders' (n 55).

61 Gorwa, 'Stakeholders' (n 55).

62 Reproduced with permission from Gorwa, 'Stakeholders' (n 55), 503.

Table 2: Stakeholders in the politics of DSA systemic risks[63]

Internal politics	*External politics*	
VLOPs	**Public authorities**	**External stakeholders**
Executives	The European Commission / DG Connect	Auditors, consultants and software providers
Shareholders	National digital services coordinators (DSCs)	NGOs
Legal staff	Courts	Academic researchers / institutions
Trust and safety staff	Law enforcement/security agencies	Media
Engineers / product design staff		

3.1 The Internal Politics of VLOPs

VLOPs hold the primary responsibility for producing risk assessments and implementing mitigation measures. They are thus directly responsible for deciding what constitutes a risk, and how particular risks should be defined, assessed and mitigated. This enables them not only to select specific compliance measures, but also to set the agenda for broader regulatory policy debates.[64] As detailed in sections 3.2 and 3.3, these processes are overseen by regulators and external stakeholders. However, VLOPs' 'first-mover advantage' and direct control over risk management processes will accord them significant power to set the agenda for the broader expert community, by highlighting issues, producing data, and formulating problem framings, proposed solutions and success metrics to which other stakeholders must then respond.[65]

3.1.1. Competing Goals and Sub-Firm Constituencies

All VLOPs but one (Wikipedia) are for-profit corporations.[66] At a general level, then, their decisions on risk management – as in any other area – will be guided by straightforward economic incentives: maximizing growth, profit

63 Author's own elaboration.

64 Kevin Wei and others, 'How Do AI Companies "Fine-Tune" Policy? Examining Regulatory Capture in AI Governance' (2024) arXiv https://arxiv.org/abs/2410.13042 accessed 22 January 2025.

65 Beatriz Botero Arcila, 'Systemic Risks in the DSA and its Enforcement' (*DSA Decoded*, 2024) www.dsadecoded.com/systemic-risks-in-the-dsa-and-its-enforcement accessed 22 January 2025.

66 European Commission, 'Supervision of the designated very large online platforms and search engines under DSA' (18 October 2024) https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses accessed 31 March 2025.

and shareholder value.[67] However, to analyze how the DSA's risk management obligations are translated into practice, a 'simplified view of coherent, bounded, successful profit maximizers' is inadequate.[68] Understanding the context-dependent decision-making processes involved and the interactions between VLOPs and other stakeholders requires 'seeing [companies] as complex, internally divided organizational entities, subject to contradictory priorities and agendas'.[69] This is relevant to systemic risk management for two particular reasons.

First, maximizing profits and share value involves different, sometimes conflicting goals. On the one hand, VLOPs are generally incentivized to minimize regulatory compliance costs as far as possible.[70] However, this must be balanced against countervailing incentives – most obviously, the risk of legal liability if the Commission deems their DSA compliance inadequate.[71] However, VLOPs also have other commercial incentives to invest in risk management. These include reputational pressure to be seen to be conducting business responsibly – both by the general public and mainstream media,[72] and by important business partners such as advertisers[73] – and the need to maintain a positive user experience.[74] In effect, many potential systemic risks, such as disinformation, spam and fraud, or online harassment, are also bad for business, and thus simultaneously constitute commercial risks to be managed. Evidently, these various goals can be operationalized, prioritized and balanced in different ways. As such, what constitutes an optimal risk management strategy for any given VLOP is open to different interpretations.

---

67 Ioannis Lianos, 'Value Extraction and Institutions in Digital Capitalism: Towards a Law and Political Economy Synthesis for Competition Law' (2023) 1 European Law Open 852 https://doi.org/10.1017/elo.2023.2; Lucian A Bebchuk, Kobi Kastiel and Anna Toniolo, 'How Twitter Pushed Stakeholders under the Bus' (2023) 28 Stanford Journal of Law, Business & Finance 307.

68 Devika Narayan, 'The Political Economy of Digital Platforms: Key Directions' (2024) 1 Platforms & Society 1, 3 https://doi.org/10.1177/29768624241263071.

69 Narayan (n 68) 3. See also Power, 'Risk Management of Nothing' (n 49); Gorwa, 'Stakeholders' (n 55).

70 Kate Klonick, 'The End of the Golden Age of Tech Accountability' (*The Klonickles*, 3 March 2023) https://klonick.substack.com/p/the-end-of-the-golden-age-of-tech accessed 22 January 2025. Importantly, this is the case even for companies like Meta, Amazon or Microsoft which have vast resources available: the imperative of shareholder value maximization still creates a strong pressure to cut costs.

71 The potential costs here could be quite high, at up to 6% of their worldwide annual turnover: see Art 52(3), DSA (n 1).

72 Nahema Marchal and others, 'How Negative Media Coverage Impacts Platform Governance: Evidence from Facebook, Twitter, and YouTube' (2024) Political Communication https://doi.org/10.1080/10584609.2024.2377992.

73 Rachel Griffin, 'From Brand Safety to Suitability: Advertisers in Platform Governance' (2024) 12(3) Internet Policy Review https://doi.org/10.14763/2023.3.1716.

74 Klonick, 'New Governors' (n 54).

Second, within a complex organization like a multinational tech company, different 'sub-firm constituencies' have different perspectives and priorities.[75] How VLOPs implement risk management in practice will depend on negotiations and compromises between internal constituencies with different goals and priorities, and on their relative influence on the company's overall strategy. That will in turn be influenced by external pressures, such as liability risks and input from other stakeholder groups.

In general, CEOs and other senior executives have the most decision-making power within a company. Indeed, commentators have pointed out that leading platform companies are characterized by an unusually high concentration of decision-making power with individual CEOs.[76] The DSA clearly envisages that senior executives should oversee the management of systemic risks: Article 41(1) requires VLOPs to establish a 'compliance function' headed by a senior executive who reports directly to the company's top management, while Articles 41(5) and (6) require top managers to oversee and sign off on the company's risk management strategy. More generally, by setting overall business strategies and priorities, senior executives will determine the conditions under which lower-level staff work on risk management, and the resources available for different aspects of this work. As described above, these management strategies may be influenced by a number of competing priorities and business objectives. However, at a general level it can be observed that senior executives' decisions tend to be heavily if not exclusively focused on maximizing profits and shareholder returns, often at the expense of other considerations, such as corporate social responsibility commitments.[77]

Shareholders can therefore be identified as another important stakeholder group, since they have significant indirect influence on risk management. Not only are executives legally required to act in the interests of shareholders;[78] the interests of the two groups are generally aligned, since company shares typically make up a high proportion of senior executives' compensation.[79] Consequently, although shareholders would rarely if ever directly participate

---

75 Gorwa, 'Stakeholders' (n 55), 499. See also Chinmayi Arun, 'Facebook's Faces' (2021) 135 Harvard Law Review 236; Narayan (n 68).

76 For example, Meta and Google are public companies but have dual-class share structures in which the founders have more voting rights than other shareholders, while X (formerly Twitter) is now a private company majority-owned by Elon Musk: Julie E Cohen, 'Oligarchy, State and Cryptopia' (forthcoming 2025) 94 Fordham Law Review https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5171050 accessed 31 March 2025; Paddy Leerssen, 'The Political Economy of Content Moderation' (draft article on file with author).

77 Bebchuk and others (n 67).

78 While the extent to which managers are obliged to act *exclusively* in the interests of shareholders is debated, and varies between jurisdictions, it is to shareholders that company executives are ultimately accountable: Edward B Rock, 'For Whom is the Corporation Managed in 2020? The Debate over Corporate Purpose' (2020) ECGI Working Papers 515/2020, 10 September 2020 https://www.ecgi.global/publications/working-papers/for-whom-is-the-corporation-managed-in-2020-the-debate-over-corporate accessed 31 March 2025.

79 Bebchuk and others (n 67).

in risk management decisions,[80] their interests and preferences significantly influence VLOPs' overall business strategies.[81] In turn, this influences regulatory compliance and risk management, for example by determining the level of resources allocated for risk mitigation measures. As an illustration of this, when several VLOPs laid off numerous 'trust and safety' and content moderation staff in 2023, this led to a jump in share prices.[82] This was widely perceived not just as a consequence of the layoffs but as their primary motivation, as a way to 'extract the kind of cost savings that Wall Street loves'.[83]

At a more granular intra-organizational level, legal staff play a significant role in shaping how companies approach regulatory compliance. Sociolegal research on legal compliance work in related fields, such as privacy and data protection, depicts a complex and ambivalent position within companies.[84] Legal staff may be strongly motivated to comply with both the letter and spirit of the law, not only because of liability risks, but also due to normative commitments to privacy, user safety, corporate social responsibility and so on. At the same time, however, their work tends to favor understandings of risk that align with business objectives, often focusing on formalistic compliance procedures over substantive changes to business practices.

Finally, in the context of platform governance, risk management also heavily involves staff working in 'trust and safety' – a now well-established professional field, encompassing various kinds of policy, cybersecurity, content moderation and product design work aimed at preventing behavior deemed harmful to a platform's users, reputation and/or commercial incentives.[85] As Kate Klonick shows, because of the commercial pressures discussed above,

---

80 Shareholder influence may sometimes involve individual 'activist investors' explicitly seeking to influence business strategies, but 'big tech' shares are heavily held by the 'big three' asset management firms and other large institutional investors: Antoine Michon and Paul-Adrien Hippolite, Big Tech Dominance (1): *The New Financial Tycoons* (Fondation pour l'innovation politique, December 2018) www.fondapol.org/en/study/big-tech-dominance-1-the-new-financial-tycoons/ accessed 25 December 2024. The latter groups typically do not participate very actively in business decisions, but to the extent that they do, they have (unsurprisingly) tended to favor profit maximization over other goals such as corporate social responsibility commitments: Benjamin Braun, 'Exit, Control, and Politics: Structural Power and Corporate Governance under Asset Manager Capitalism' (2022) 50(4) Politics & Society 630 https://doi.org/10.1177/00323292221126262.

81 Paddy Leerssen, 'Political Economy' (n 76).

82 Subrat Patnaik and Ryan Vlastelica, 'Big Tech's Job Cuts Spur Rallies Even as an Economic Slowdown Looms' (*Bloomberg*, 25 January 2023) www.bloomberg.com/news/articles/2023-01-25/big-tech-s-job-cuts-spur-rallies-even-as-economic-slowdown-looms accessed 26 September 2024.

83 Andrew Ross Sorkin and others, 'Technology Companies Are Cutting Jobs and Wall Street Likes It' (*The New York Times*, 30 January 2024) www.nytimes.com/2024/01/30/business/dealbook/tech-layoffs.html accessed 31 March 2025.

84 Bamberger and Mulligan (n 51); Lauren Edelman, *Working Law: Courts, Corporations and Symbolic Civil Rights* (University of Chicago Press, 2016); Ari Ezra Waldman, 'Privacy Law's False Promise' (2020) 97 Washington University Law Review 773; Ari Ezra Waldman, *Industry Unbound: The Inside Story of Privacy, Data, and Corporate Power* (CUP 2022).

85 Elena Cryst and others, 'Introducing the Journal of Online Trust and Safety' (2023) 1 Journal of Online Trust & Safety 1; Graham Denyer Willis, ''Trust and Safety': Exchange, Protection and the Digital Market–Fortress in Platform Capitalism' (2023) 21 Socio-Economic Review 1877 https://doi.org/10.1093/ser/mwad003; Tom R Tyler, Tracey Meares and Matt Katsaros, 'New Worlds Arise: Online Trust and Safety' (2025) 8 Annual Review of Criminology https://doi.org/10.1146/annurev-criminol-111523-122337.

platforms have invested significantly in building up trust and safety departments whose work goes far beyond what is strictly legally required.[86] This has effectively created sub-firm constituencies with their own goals (eg prioritizing user safety, even if this means compromising on other commercial objectives) and institutional incentives (eg attracting more resources and responsibility). Many risk areas and possible mitigation measures listed in Articles 34–35 (eg content moderation, child protection, cooperation with trusted flaggers, development of codes and policies) traditionally fall under the responsibility of trust and safety teams, who will thus play a major role in risk management in practice. Their influence, however, will ultimately depend on how effectively they can advocate for their own goals and priorities as against those of other teams, which may be more focused on growth and revenue.

3.1.2. Internal Conflicts

How these processes play out in practice will probably be very context-specific – differing both between different VLOPs, and between different policy issues and risk areas. However, several points can be highlighted which are of general relevance, and which could point to interesting areas for future research.

First, trust and safety has become increasingly institutionalized as a professional specialism and expert community[87] – with two professional associations[88] and various informal networks and groups.[89] Trust and safety has also become a thriving academic subfield with its own journal[90] and annual conference (the ironically named TrustCon[91]). This institutionalization may strengthen the authority accorded to trust and safety staff inside VLOPs, by giving them the status of professional experts, and enabling them to advocate for best practices that are widely recognized as such. At the same time, this professionalization may also increase VLOPs' influence on how other stakeholders understand systemic risks. Due to their resources and recognized technical expertise, large companies' legal and compliance staff can significantly influence how external actors understand and implement regulation.[92] Platform staff already enjoy a certain authority in the broader DSA expert community: for example, conferences and events typically include academics and civil society

---

86 Klonick, 'New Governors' (n 54).

87 Tyler and others (n 85).

88 Integrity Institute, 'We Protect the Social Internet' https://integrityinstitute.org/ accessed 22 January 2025; Trust & Safety Professional Association, 'Advancing the Trust and Safety Profession through a Shared Community of Practice' www.tspa.org/ accessed 22 January 2025.

89 Denyer Willis (n 85).

90 Cryst and others (n 85).

91 TrustCon, 'TrustCon 2025: Jul 21-23' (*TrustCon* 2025) www.trustcon.net/event/0f932abb-fad0-4e42-a1b7-7563f6123e41/summary accessed 22 January 2025.

92 Waldman, 'False Promise' (n 84); Ari Ezra Waldman, 'Privacy, Practice and Performance' (2022) 110 California Law Review 1221.

and industry professionals, blurring the boundaries between actors with rather different professional norms and incentives. The professionalization of trust and safety may thus help VLOPs' staff build consensus around understandings of systemic risks, and appropriate mitigation measures, that are friendly to their employers' interests.

Second, from a new governance perspective, regulations like the DSA aim to strengthen the negotiating position of those sub-firm constituencies whose goals align with the objectives of the regulatory regime.[93] For example, Article 34 risk assessments effectively establish formal channels for trust and safety and compliance staff to assess and evaluate other teams' activities, as well as enabling them to point to potential legal or reputational costs if their advice is ignored. Article 41's requirements for an independent compliance function are presumably envisaged as a way of creating a stronger internal constituency advocating for risk mitigation, which functions somewhat independently from the company's commercial objectives.

Third, however, staff working within a for-profit company can never be fully insulated from commercial considerations. Legal or trust and safety staff may advocate for particular risk mitigation measures and priorities that conflict with their employer's revenue and profit goals, but they generally cannot suggest fundamental changes to its business model or strategy. Their capacities and influence will also be limited by resource constraints. Journalistic reporting and leaks consistently depict trust and safety teams at even the largest and wealthiest VLOPs as overstretched and understaffed.[94] Additionally, many possible risk mitigation measures will require cooperation from other teams, who will themselves have limited resources and conflicting priorities, and may therefore resist demands from trust and safety or compliance staff. For example, anything involving changes to interface design or software infrastructures will require work from highly-qualified software engineers and data scientists, who are – from the company's perspective – a scarce resource, with many other demands on their time. Finally, more senior executives may also veto

---

93 Bamberger and Mulligan (n 51); Kenneth A Bamberger, 'Regulation as Delegation: Private Firms, Decisionmaking, and Accountability in the Administrative State' (2006) 56 Duke Law Journal 377.

94 See, eg, Julia Carrie Wong, 'How Facebook Let Fake Engagement Distort Global Politics: A Whistleblower's Account' (*Guardian*, 12 April 2021) www.theguardian.com/technology/2021/apr/12/facebook-fake-engagement-whistleblower-sophie-zhang accessed 18 January 2023; Justin Scheck, Newley Purnell and Jeff Horwitz, 'Facebook Employees Flag Drug Cartels and Human Traffickers. The Company's Response Is Weak, Documents Show' (*Wall Street Journal*, 16 September 2021) www.wsj.com/articles/facebook-drug-cartels-human-traffickers-response-is-weak-documents-11631812953 accessed 18 January 2023; Donie O'Sullivan, Clare Duffy and Brian Fung, 'Ex-Twitter Exec Blows the Whistle, Alleging Reckless and Negligent Cybersecurity Policies' (CNN, 23 August 2022) https://edition.cnn.com/2022/08/23/tech/twitter-whistleblower-peiter-zatko-security/index.html accessed 18 January 2023; Jason Koebler, 'Where Facebook's AI Slop Comes From' (*404 Media*, 6 August 2024) www.404media.co/where-facebooks-ai-slop-comes-from/ accessed 26 September 2024.

risk mitigation measures proposed by trust and safety teams if they are felt to undermine the company's overall strategic goals.[95]

Moreover, beyond any direct conflicts, if trust and safety is not a priority for senior management, then the area may simply be structurally sidelined – so that their activities signal the company's commitment to DSA compliance to regulators and other stakeholders, but have limited impact on the work of other departments. Waldman observes this dynamic within many tech companies: privacy staff implement policies and procedures that are largely treated as a formality by teams working on product design, data processing, and so on, and have little impact on how they actually treat users' data.[96] Similarly, Thomas Tyler, Tracey Meares and Matt Katsaros (a former Twitter and Meta employee) note that trust and safety teams are often not well integrated with teams working on product design, which could limit the former's influence on consequential design decisions.[97]

More generally, sociolegal scholarship on regulatory compliance has highlighted that 'cosmetic compliance' or 'box-checking' approaches to compliance are more likely where legal rules are vague and ambiguous, where standards and guidance come from many different sources, and where companies' internal processes are not transparent to the public[98] – all factors which are very present in the DSA.[99] While it is too early to say how much these 'cosmetic compliance' dynamics will ultimately shape DSA systemic risk management, arguably some signs can already be seen in VLOPs' first risk assessment reports.[100] Commentators have observed a tendency for VLOPs to construct risks in terms of external threats from 'bad actors', rather than as potential harms resulting

---

95 Mark Bergen, 'YouTube Executives Ignored Warnings, Letting Toxic Videos Run Rampant' (*Yahoo Finance*, 2 April 2019) https://finance.yahoo.com/news/youtube-executives-ignored-warnings-letting-090026613.html?guccounter=1 accessed 11 January 2023; Karen Hao, 'How Facebook got Addicted to Spreading Misinformation' (*MIT Technology Review*, 11 March 2021) www.technologyreview.com/2021/03/11/1020600/facebook-responsible-ai-misinformation/ accessed 3 January 2022; Jeremy B Merrill and Will Oremus, 'Five Points for Anger, One for a "Like": How Facebook's Formula Fostered Rage and Misinformation' (*Washington Post*, 26 October 2021) www.washingtonpost.com/technology/2021/10/26/facebook-angry-emoji-algorithm/ accessed 3 January 2022.

96 Waldman, 'False Promise' (n 84); Waldman, *Industry Unbound* (n 84).

97 Tyler and others (n 85).

98 Edelman (n 84); Ingrid Landau, 'Human Rights Due Diligence and the Risk of Cosmetic Compliance' (2019) 20(1) Melbourne Journal of International Law 221.

99 Rachel Griffin, 'Rethinking Rights in Social Media Governance: Human Rights, Ideology and Inequality' (2023) 2(1) European Law Open 30 https://doi.org/10.1017/elo.2023.7.

100 These reports (which include a summary of a VLOP's risk assessments, the audit report required under Art 37 DSA, and the VLOP's response to the audit report) were submitted to DG Connect in 2023 but first released to the public in late 2024. For an overview, see Alexander Hohlfeld, 'DSA Risk Assessment & Audit Database' (*Google Docs*, 24 January 2025) https://docs.google.com/spreadsheets/d/12hJWpCFmHJMQQlz1qkd6OgGsMW82YcsWgJHXD7BHVps/edit?gid=0#gid=0 accessed 27 March 2025.

from their own business practices and priorities.[101] They also focus much more on describing pre-existing content moderation and safety measures, and reframing these in terms of systemic risk mitigation, rather than evidencing concrete changes made in response to risk assessments.[102]

Finally, at the time of finalizing this article in April 2025, there is a general trend across major platforms to cut spending on trust and safety and compliance, and to more aggressively resist potentially-costly regulation.[103] Arguably already visible since the 2023 wave of layoffs discussed above,[104] this shift has noticeably intensified since the 2024 US election: several US-based 'big tech' firms have explicitly positioned themselves as allies of the second Trump administration and its reactionary, ethnonationalist and protectionist political agenda, and have sought its support in opposing EU platform regulation initiatives, including the DSA.[105] This situation is also shaping internal politics and strategic priorities within companies, in ways that are highly relevant to DSA systemic risk management. VLOPs have already moved to reduce the relative influence and resources of compliance teams[106] and to scale down risk mitigation measures such as fact-checking programs.[107] Overall, in the current political climate, it seems likely that internal constituencies pushing for more substantial risk mitigation measures will generally not be in a strong position, and that VLOPs' business strategies will instead favor minimizing costs through tactics like 'cosmetic compliance'.

---

[101] DSA Civil Society Coordination Group, *Initial Analysis on the First Round of Risk Assessment Reports under the EU Digital Services Act* (Center for Democracy & Technology, March 2025) https://cdt.org/wp-content/uploads/2025/03/RA-Report-Assessment-Report.pdf accessed 27 March 2025.

[102] For example, Meta's report for Facebook dedicates 41 pages to a detailed presentation of its existing 'ecosystem of controls' and how they mitigate DSA systemic risks, with only occasional references to where it has identified 'areas for continued improvement'. The latter typically involve fine-tuning of existing tools and policies, and responding to changing circumstances and external 'threat actors', rather than implementing novel risk mitigation measures or significant operational changes. There is one page detailing concrete changes that Meta made as a result of the risk assessment. See Meta, *Regulation* (EU) 2022/2065 *Digital Services Act (DSA) Systemic Risk Assessment and Mitigation Report for Facebook* (Meta, August 2024), 45–88 https://scontent-ber1-1.xx.fbcdn.net/v/t39.8562-6/468433223_2965672840272736_5366479269132269710_n.pdf accessed 27 March 2025.

[103] Tech companies have always invested heavily in lobbying efforts aimed at influencing such regulations so that they accommodate business interests: Corporate Europe, 'Big Tech's Last Minute Attempt to Tame EU Tech Rules: Lobbying in Times of Trilogues' (23 April 2022) https://corporateeurope.org/en/2022/04/big-techs-last-minute-attempt-tame-eu-tech-rules accessed 23 January 2025; Corporate Europe, 'Byte by Byte: How Big Tech Undermined the AI Act' (17 November 2023) https://corporateeurope.org/en/2023/11/byte-byte accessed 23 January 2025. However, they are now shifting towards more confrontational strategies and open opposition to EU regulatory efforts: Théophane Hartmann, 'US Tech Moguls Slam EU Digital Rulebook' (*Euractiv*, 13 January 2025) www.euractiv.com/section/politics/news/us-tech-moguls-slam-eu-digital-rulebook/ accessed 31 March 2025.

[104] Klonick, 'Golden Age' (n 70).

[105] Nilay Patel and Kate Klonick, 'How Meta's MAGA Heel Turn is a Play for Global Power' [Audio podcast] (*The Verge*, 23 January 2025) www.theverge.com/24349734/meta-trump-free-speech-big-tech-power-geopolitics-zuckerberg-elon-musk-decoder-podcast-interview accessed 31 March 2025.

[106] Kalley Huang, 'Meta Curbs Privacy Teams' Sway Over Product Releases' (*The Information*, 11 February 2025) www.theinformation.com/articles/meta-curbs-privacy-teams-sway-over-product-releases accessed 31 March 2025.

[107] Anupriya Datta, 'US Big Tech Backtracks on EU Fact-Checking Commitments' (*Euractiv*, 22 January 2025) www.euractiv.com/section/tech/news/us-big-tech-backtracks-on-eu-fact-checking-commitments/ accessed 31 March 2025.

3.2 State Institutions and Regulatory Oversight

Although VLOPs exercise significant power to shape systemic risk management, this process takes place within a binding legal framework. This means that what constitutes adequate risk management is ultimately a decision for state institutions. In particular, the Commission holds the primary enforcement responsibility.[108] However, it is not the only relevant body. Courts could play a significant role in interpreting relevant legal provisions (particularly important given that Articles 34–35 are so open to different interpretations). National agencies could also exercise significant agenda-setting power, even without the authority to issue binding legal interpretations.

3.2.1. The European Commission

The Commission has exclusive competence to enforce those DSA provisions which apply only to VLOPs, most importantly the systemic risk framework (it also has joint competence with the relevant national regulators for enforcing other, generally-applicable provisions against VLOPs: see Article 56). It has set up a specialist DSA enforcement team based within the Directorate-General for Communications Networks, Content and Technology (DG Connect).[109]

Ultimately, if it finds that a VLOP is not complying with its risk management obligations, the Commission can impose fines of up to 6% of the company's worldwide annual turnover.[110] Importantly, however, it can also influence how VLOPs approach risk management through several less drastic mechanisms – both at a general level, and in relation to specific VLOPs. In this regard, the DSA seems to take inspiration from 'responsive regulation' approaches, in which regulators first attempt to achieve policy objectives through dialogue and cooperation with companies, only escalating towards more coercive enforcement if this approach fails.[111]

---

[108] Art 56(2), DSA (n 1).

[109] European Commission, 'Do you want to help enforce the Digital Services Act? Apply now to be part of the DSA enforcement team!' (15 January 2024) https://digital-strategy.ec.europa.eu/en/news/do-you-want-help-enforce-digital-services-act-apply-now-be-part-dsa-enforcement-team accessed 22 January 2025.

[110] Art 52(3), DSA (n 1).

[111] Ian Ayres and John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (OUP 1992). In line with this approach, DG Connect's director of platform policy has stated that the Commission will prioritize dialogue with VLOPs and voluntary commitments over formal enforcement where possible: Rita Wezenbeek, 'Opening Keynote - The European Commission and the DSA' (DSA and Platform Regulation Conference, Amsterdam, 16 February 2024) https://dsa-observatory.eu/the-dsa-and-platform-regulation-conference-2024/ accessed 23 October 2024.

First, at a general level, DG Connect can issue official guidance on the management of specific risks.[112] For example, in 2023 it commissioned and published a model risk assessment on risks of Russian disinformation.[113] As provided by Article 37(7), it has also issued a delegated act setting out guidance on auditing methodologies and independence requirements.[114] Finally, Articles 45–47 provide for VLOPs and other industry and civil society stakeholders to draw up codes of conduct with more concrete guidance on risk mitigation. The Commission will have significant input into these drafting processes, as it can provide instructions and invite specific stakeholders to participate.[115]

The Commission can also influence individual VLOPs' risk management strategies through discussions and advice – ultimately backed, of course, by the threat of investigations and fines. Any enforcement action would be preceded by investigatory measures, including formal requests for information,[116] demands for internal documents and data,[117] and interviews and on-site inspections.[118] VLOPs threatened with enforcement proceedings can also offer voluntary commitments, which the Commission can choose to accept and make binding, or reject as insufficient for compliance.[119] Finally, before any formal non-compliance decision, the Commission should communicate preliminary findings to the VLOP in question, and explain how the non-compliance could be rectified; if the VLOP agrees to this, the investigation can be closed.[120]

These various mechanisms will give the Commission frequent opportunities to signal to VLOPs – and to other stakeholders and observers – what kinds of risks it is concerned about, how it thinks these risks should be understood and mitigated, and what kinds of issues might ultimately lead to enforcement proceedings. For example, as of April 2025, the Commission has initiated only 10 enforcement proceedings, but has issued 66 requests for information from 23 of the 25 designated VLOPs.[121] These requests are confidential, but they are accompanied by public press releases which indicate which DSA provisions, risks and mitigation measures are involved, and which therefore give

---

[112] Art 35(3), DSA (n 1).

[113] European Commission, *Risk management framework* (n 2); European Commission, "Guidelines for providers" (n 3).

[114] Commission Delegated Regulation (EU) 2024/436 of 20 October 2023 supplementing Regulation (EU) 2022/2065 of the European Parliament and of the Council, by laying down rules on the performance of audits for very large online platforms and very large online search engines [2024] OJ L.

[115] Griffin, 'Codes of Conduct' (n 5).

[116] Art 67, DSA (n 1).

[117] Arts 40 and 72, DSA (n 1).

[118] Arts 68-69, DSA (n 1).

[119] Art 71, DSA (n 1).

[120] Art 73, DSA (n 1).

[121] European Commission, 'Supervision' (n 66).

some idea of the Commission's enforcement priorities.[122] Presumably, VLOPs will factor this information into their approach to compliance. The voluntary commitments procedure has also already been used once: TikTok committed not to launch its TikTok Lite app in the EU after DG Connect initiated an investigation and expressed a clear view that the app's gamification features posed unacceptable risks to minors' mental health.[123]

Finally, instead of or in parallel with these formal procedures, the Commission can also communicate expectations to platforms using less formal channels – either through public statements (such as Breton's open letters), or in private conversations between staff and policymakers at various levels.[124] In this regard, civil society commentators have expressed concerns about the possibility that Commission staff and politicians could encourage platforms to restrict users' freedom of expression through informal and opaque channels.[125]

Like VLOPs, the Commission has its own internal differences. It was widely rumored in the DSA expert community that many lower-level Commission staff had criticized Breton's open letters to platforms, backing up the concerns about freedom of expression raised by civil society.[126] More generally, however, beyond such open conflicts, the Commission's enforcement strategies will inevitably reflect discussions and negotiations between different levels and departments of the organization. As of 2024, DG Connect is under the responsibility of the Vice-President for Tech Sovereignty, Security and Democracy, Henna Virkkunen; however, some aspects of DSA enforcement fall within the briefs of justice commissioner Michael McGrath and internal market commissioner Stéphane Séjourné.[127] These Commissioners may have different views on how the DSA should be enforced, and how DSA enforcement should be balanced against other priorities. Moreover, while Commissioners can set high-level strategies and priorities, civil servants within DG Connect will decide how particular risks should be defined and measured, how to communicate with VLOPs and other stakeholders, and when to initiate investigations or enforcement actions. Many of these staff will be career civil servants, but

---

[122] Botero Arcila (n 65).

[123] European Commission, 'TikTok commits to permanently withdraw TikTok Lite Rewards programme from the EU to comply with the Digital Services Act' (European Commission Press Corner, 5 August 2024) https://ec.europa.eu/commission/presscorner/detail/en/ip_24_4161 accessed 22 January 2025. For a detailed analysis of this enforcement process see Fornasari and Griffin (n 38).

[124] Keller (n 46); Global Network Initiative & Digital Trust & Safety Partnership, *European Rights & Risks: Stakeholder Engagement Forum Event Summary* (Global Network Initiative 2024) https://globalnetworkinitiative.org/wp-content/uploads/GNI-DTSP-Forum-Summary.pdf accessed 23 October 2024.

[125] Keller (n 46); Jordi Calvet-Badamunt, 'TikTok has Permanently Withdrawn the TikTok Lite Rewards Program from the EU. This is a Worrying Development.' (*Bluesky*, 5 August 2024) https://bsky.app/profile/jordicalbad.bsky.social/post/3kyyt6fbifk2t accessed 22 January 2025.

[126] DSA Decoded (n 12).

[127] European Commission, 'Commissioners-designate (2024-2029)' (17 September 2024) https://commission.europa.eu/about/commission-2024-2029/commissioners-designate-2024-2029_en accessed 22 January 2025.

DG Connect has also hired a number of academics specializing in platform regulation to work on DSA enforcement. Staff with different professional backgrounds and political views may have quite different views about what the most important risks are and how they should be managed.

3.2.2. Digital Services Coordinators

National regulatory agencies, or 'digital services coordinators' (DSCs), [128] will play a secondary but still important role in the construction of systemic risks. In particular, they will exercise influence through the European Board for Digital Services (EBDS), which brings together representatives of all the designated DSCs for regular meetings, chaired by the Commission. In these discussions, individual DSCs, and coalitions of DSCs with similar views, can advocate for their preferred understandings of risk, political priorities, and monitoring and enforcement strategies. Although the EBDS is not directly responsible for enforcement, it is supposed to generally advise and assist the Commission. [129] It must also publish a yearly report identifying 'the most prominent and recurrent systemic risks' relating to multiple VLOPs, as well as recommending best practices for risk mitigation, [130] and should help oversee codes of conduct. [131] These assessments could significantly shape how the Commission approaches enforcement, and how VLOPs approach compliance.

More generally, the EBDS and individual DSCs could play an influential coordinating and agenda-setting role in the wider DSA expert community, by commissioning research or advocating for their own policy priorities. For example, Articles 62(5) and (6) provide that the EBDS can invite external experts and stakeholders to meetings, and run its own public consultation processes. Article 63(1)(e) gives it a broad mandate to 'promote the development and implementation of European standards, guidelines, reports, templates and code of conducts [sic] in cooperation with relevant stakeholders'. DSCs (in particular those from larger member states and from northern and western Europe [132]) are well-represented at conferences and other specialist events, and some have signaled their intention to participate actively in policy debates

---

[128] Member states can divide different aspects of DSA enforcement among multiple agencies, but must nominate one as a 'digital services coordinator' (DSC), responsible for overseeing the work of other national agencies as well as liaising internationally with the Commission and other member states' DSCs: see Arts 49–51, DSA (n 1). This subsection focuses on DSCs because, given the EU-wide scope of the systemic risk framework and the centralization of enforcement, their responsibility for international coordination will give them a larger role in systemic risk management than other member state agencies. However, as section 3.2.3 notes, other national agencies could also influence broader policy discourse around systemic risks.

[129] See Arts 61(2)(c) and 63(1)(d), DSA (n 1).

[130] Art 35(2), DSA (n 1). At the time of finalizing this article in April 2025, the EBDS is in the process of drafting the first such report, which will cover the period from February 2024 to February 2025: personal communication to the author, DG Connect, 20 March 2025.

[131] Arts 45-47, DSA (n 1).

[132] Jennifer Orlando-Salling, 'The Digital Services Act in the European Periphery: Critical Perspectives on EU Digital Regulation' (2025) 3(4) European Law Open 849 https://doi.org/10.1017/elo.2024.52

around systemic risks. For example, in 2024, Germany's Bundesnetzagentur commissioned four academic studies into various aspects of the identification, analysis, mitigation and social impacts of DSA systemic risks. [133]

Finally, DSCs with responsibility for other legal provisions that overlap with the (very broad) scope of Articles 34–35 could also indirectly impact how VLOPs approach risk mitigation. VLOPs attempting to minimize costs will generally want to streamline and standardize regulatory compliance processes – for example, by aligning the measures they take to comply with different regulatory frameworks. [134] This suggests that member state DSCs enforcing legislation dealing with similar topics (as well and regulatory agencies in other jurisdictions with similar legislation, such as the UK's 2023 Online Safety Act) could significantly shape how VLOPs approach compliance with Articles 34-35 DSA.

In this regard, Ireland's Media Commission (CnaM) is likely to be particularly influential, as 15 of the 25 VLOPs are based in Ireland, and therefore need to comply with all applicable Irish regulations. [135] Notably, CnaM is responsible for developing codes of conduct implementing Article 28b of the 2018 updated Audiovisual Media Services Directive, which requires 'video-sharing platforms' – a category that covers most social media platforms, including the VLOPs Facebook, Instagram, TikTok, YouTube, X and LinkedIn [136] – to mitigate risks associated with certain types of illegal content, such as hate speech, and with children encountering harmful content more generally. Its scope thus overlaps substantially with that of Articles 34–35 DSA. CnaM's first Online Safety Code, issued in 2024, prescribes a number of risk mitigation measures, including age verification measures and parental controls, as well as specific types of content that companies must ban in their terms and conditions. [137] VLOPs who are required to implement these measures in any case are also likely to incorporate them into their DSA compliance processes, and present them as systemic risk mitigation measures.

---

[133] Bundesnetzagentur, 'Ausschreibungen' www.bundesnetzagentur.de/DE/Allgemeines/DieBundesnetzagentur/BeschaffungAusschreibungen/start.html accessed 1 July 2024.

[134] Global Network Initiative & Digital Trust & Safety Partnership (n 124).

[135] European Commission, 'Supervision' (n 66).

[136] Coimisiún na Meán, 'Coimisiún na Meán designates Video-Sharing Platform Services' (9 January 2024) www.cnam.ie/coimisiun-na-mean-designates-video-sharing-platform-services/ accessed 27 January 2025.

[137] Coimisiún na Meán, 'Online Safety Code' (October 2024) www.cnam.ie/app/uploads/2024/11/Coimisiun-na-Mean-Online-Safety-Code.pdf accessed 6 May 2025.

3.2.3. Courts

While the DSA is primarily enforced by regulatory agencies, courts have ultimate authority to rule on its interpretation. By their nature, such determinations will involve cases where stakeholders disagree with one another, and where the outcomes of these conflicts are sufficiently uncertain and significant to make it worth going to court. Courts could thus resolve some of the most contentious questions about systemic risk management.

This could involve litigation focusing directly on Articles 34–35 – for example, if a VLOP fined for non-compliance challenges the Commission's decision.[138] However, this is not the only possible legal route. Article 40(4) provides that national DSCs should authorize vetted researchers to access VLOPs' internal data 'for the sole purpose of conducting research that contributes to the detection, identification and understanding of systemic risks in the Union'. Article 40(12) further requires VLOPs to facilitate access to data that is already publicly accessible on their platforms (for example, by permitting scraping or providing research APIs) for research with these purposes. If DSCs refuse vetted researcher status, or VLOPs refuse access to public data, on the grounds that the research in question does not involve relevant systemic risks, researchers could challenge such decisions in court and argue that their research does in fact relate to a systemic risk. Conversely, VLOPs could also challenge the grant of vetted researcher status by DSCs on the grounds that the research does not involve systemic risks. Either situation would allow courts to explicitly rule on the scope of Article 34.[139] Finally, national courts may take DSA obligations into account in cases against VLOPs that are primarily based on other grounds (for example, to inform the definition of a duty of care under tort law, an abuse of power under competition law, or a fair balance between the parties' interests under contract law[140]). Such cases could also provide influential, albeit non-binding, guidance on the interpretation of Articles 34–35.

These multiple legal routes raise complicated jurisdictional questions which cannot be fully explored here, but as a general point, courts at both EU and national levels could be involved. As a regulation, the DSA is directly en-

---

[138] There have already been some legal challenges to other aspects of DSA enforcement, such as the designation of VLOPs: Linda Weigl and Aleksandra Guzik, 'In Brussels We Trust? Exploring Corporate Resistance in Platform Regulation' (2025) 17(2) Law, Innovation & Technology 335 https://doi.org/10.1080/17579961.2025.2470588.

[139] Indeed, this could enable strategic litigation by VLOPs, researchers and civil society organizations expressly seeking to contest the definition of systemic risks.

[140] Jürgen Bering and Simonetta Vezzoso, 'Meta's Fundamental Digital Rights Blunder - And a German Antitrust Fix' (Tech Policy Press, 6 August 2024) www.techpolicy.press/metas-fundamental-digital-rights-blunder-and-a-german-antitrust-fix/ accessed 7 January 2025.

forceable by national courts,[141] who could for example hear cases challenging refusals of data access by their national DSCs or by VLOPs based in their jurisdiction. However, the ECJ's role will likely be particularly influential, for two reasons. First, under Article 82(3) DSA, member state courts are barred from ruling on any questions that are the subject of enforcement decisions or proceedings by the Commission – whose decisions would, however, be subject to judicial review by the ECJ. Second, where court proceedings do not directly address the enforcement of Articles 34–35 but indirectly raise questions about the interpretation of these provisions, national courts might refer questions about DSA interpretation to the ECJ.

Court cases also present opportunities for participation and contestation by other stakeholders. As noted above, VLOPs facing enforcement actions could contest the Commission's understanding of appropriate risk management. As discussed further in section 3.3, strategic litigation can also enable external stakeholders to challenge consensus understandings of risk.[142] As a general rule, however, litigation tends to favor already-powerful actors who have the funding for legal teams and lengthy proceedings.[143] In this context, that most obviously includes VLOPs (though not exclusively: other well-resourced corporate actors, such as media companies, might also find litigation advantageous). The mere prospect of being sued by a VLOP could be a disincentive for DG Connect to act on understandings of risk which are more contested or require radical changes to VLOPs' business practices, incentivizing it instead to focus on interpretations considered less likely to be challenged in court.[144] This could also incentivize greater reliance on informal enforcement mechanisms, such as private discussions with VLOPs, over formal legal processes – which, in turn, would limit the ability of other stakeholders to contest enforcement strategies.

3.2.4. Law Enforcement and Security Agencies

Finally, while they do not have direct responsibility for enforcing Articles 34–35, it is worth briefly highlighting the role of law enforcement and security agencies. These institutions do have an important role in implementing other DSA provisions – notably by issuing orders to remove illegal content.[145] They can also submit non-binding reports about content they consider to be

[141] Article 54 provides that anyone harmed by a company's failure to comply with the DSA can sue for damages in accordance with national law. Importantly, however, only consumers can sue in their national courts; anyone using a platform in a professional capacity would have to sue in the member state where the company is based. This could be a significant barrier to cross-border enforcement, particularly in enforcement against VLOPs, given their large multinational user bases: see Bering and Vezzoso (n 140).

[142] Birkland (n 17); Lina Liedlbauer, 'Politicizing European Counter-Terrorism: The Role of NGOs' (2021) 30(3) European Security 485 https://doi.org/10.1080/09662839.2021.1947802.

[143] Cohen, *Between Truth and Power* (n 33); Katharina Pistor, *The Code of Capital: How the Law Creates Wealth and Inequality* (Princeton University Press, 2019).

[144] Fornasari and Griffin (n 38).

[145] Art 9, DSA (n 1).

illegal or incompatible with a platform's terms and conditions, which can also be facilitated by official certification as a 'trusted flagger'.[146] Illegal content is the first risk area mentioned in Article 34; other risk areas such as 'civic discourse' have also largely been construed as involving harmful content, such as disinformation.[147]

Because law enforcement agencies have a prominent role in identifying and monitoring such content, they could significantly influence how other actors understand and manage associated risks. For example, Breton's famous open letters identified the prompt removal of content reported by law enforcement as a key mitigation measure.[148] More generally, Gorwa suggests that specialized police units working on particular issues, such as child abuse – and thus recognized as experts on these risk areas – could play an influential role in lobbying platforms and other state institutions to focus on particular enforcement priorities.[149]

3.3 External Stakeholders

Unlike VLOPs and state institutions, civil society organizations (CSOs) and other external stakeholders are not directly responsible for deciding how risks should be understood and managed. In practice, however, they may exercise significant influence. In some cases, they can contest regulators' and VLOPs' approaches to risk management by imposing tangible reputational and material costs, through tactics such as litigation or public advocacy. Less directly, but importantly, they can shape public discourse and knowledge about risks, get their preferred issues onto other actors' agendas, and promote framings that favor their own interests. This is especially the case given the importance of independent expertise in shaping the construction of risks and legitimizing other actors' risk management decisions. Regulators and companies routinely rely on knowledge and evidence produced by academics, civil society and third-party companies. Moreover, risk management depends not only on knowledge production, but also on practices of *authorization* that deem some forms of knowledge and discourse more valid than others.[150] Authorization often relies heavily on scientific authority and expert consensus. Thus, external actors who are seen as authoritative within the professional community working on regulatory implementation can exercise significant influence over how risks are understood.

---

146 Art 22, DSA (n 1).

147 European Commission, Risk management framework (n 2).

148 Clothilde Goujard, 'EU Starts Investigating Meta, TikTok over Hamas Content' (*Politico*, 19 October 2023) www.politico.eu/article/eu-starts-investigating-meta-tiktok-over-hamas-content/ accessed 28 October 2024.

149 Robert Gorwa, 'Durov's Arrest and the Shadow Politics of Platform Regulation' (*Tech Policy Press*, 16 September 2024) www.techpolicy.press/durovs-arrest-and-the-shadow-politics-of-platform-regulation/ accessed 22 January 2025.

150 Amoore (n 16).

3.3.1. Auditors, Consultants and Software Providers

Although discussions of 'stakeholder engagement' in the DSA typically emphasize independent, non-commercial actors like NGOs, in fact some of the most influential external stakeholders may be for-profit companies providing services to VLOPs and regulators, such as auditors, consultants and software providers.[151] This is unsurprising: historically, the development and diffusion of risk management techniques has been driven by the technical innovations and marketing efforts of businesses offering risk management services.[152] More recently, scholars have often observed that corporate risk management and due diligence regulations are 'market-making',[153] creating 'a growing cottage industry of private auditors, consultants, and experts'.[154] Often, in effect, 'the responsibility to regulate human rights is first outsourced by states to corporations and then further outsourced to other private parties'.[155]

Such an ecosystem is already emerging around the DSA (and similar regimes in other jurisdictions).[156] It prominently includes the 'big four' auditing and consultancy firms, who are widely expected to dominate the market for Article 37 audits, and are also already providing consulting services to guide VLOPs on DSA compliance.[157] Smaller consultancies specializing in trust and safety and related compliance issues are also emerging.[158] In addition, many companies offer software tools relevant to risk management, such as AI content classification tools, software tools for manual moderation, and analytics tools to monitor risky behavior such as fraud.[159] Generally, platform companies will

---

[151] In tripartite taxonomies like Gorwa's, these stakeholders could also be classified alongside VLOPs as corporate actors. However, for the purposes of this paper, their position as external partners of VLOPs – who provide advice and resources for risk management but are not directly responsible for it – means that they have more in common with NGOs and other non-commercial stakeholders than with VLOPs themselves.

[152] Ewald (n 14).

[153] Miikka Hiltunen, 'Social Media Platforms within Internal Market Construction: Patterns of Reproduction in EU Platform Law' (2022) 23 German Law Journal 1226, 1241 https://doi.org/10.1017/glj.2022.80.

[154] Antoine Duval, 'Ruggie's Double Movement: Assembling the Private and the Public Through Human Rights Due Diligence' (2023) 41 Nordic Journal of Human Rights 279, 287 https://doi.org/10.1080/18918131.2023.2171633. See also Parfitt and Bryant (n 44).

[155] Duval (n 154) 287.

[156] Keller (n 46). Historically, some aspects of trust and safety work, such as moderation, have generally been outsourced to save costs: Sana Ahmad and Maximilian Greb, 'Automating Social Media Content Moderation: Implications for Governance and Labour Discretion' (2022) 2(2) Work in the Global Economy 176 https://doi.org/10.1332/27324172 1X16647876031174. However, industry accounts suggest that the increasingly complex regulatory landscape is leading to growth both in traditional business outsourcing companies offering trust and safety services, and in newer specialized companies: Tim Bernard, 'The Evolving Trust and Safety Vendor Ecosystem' (*Tech Policy Press*, 24 July 2023) www.techpolicy.press/the-evolving-trust-and-safety-vendor-ecosystem/ accessed 23 October 2024.

[157] Petros Terzis, Michael Veale and Noelle Gaumann, 'Law and the Emerging Political Economy of Algorithmic Audits' (2024) FAccT '24: Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency 1255 https://www.dsadecoded.com/third-party-database.

[158] Bernard (n 156); Ioan Paul Sipos, 'Mapping the Digital Services Act (DSA) Compliance Industry: Private Actors, Public Stakes' (DSA Decoded, 2025) www.dsadecoded.com/third-part-database accessed 6 May 2025.

[159] Griffin, 'Brand safety' (n 73); Bernard (n 156); Sipos (n 158).

be the main clients for such services.[160] However, regulators may themselves also outsource aspects of regulatory oversight: see for example the Commission's recent call for tenders for 'market intelligence, evidence gathering and compliance monitoring' related to DSA systemic risks.[161]

Such services will significantly shape the detailed, day-to-day work of risk management. Building software to identify or measure the prevalence of risky activities necessarily involves making contestable policy choices about how such activities should be defined.[162] Third-party vendors are thus active participants in the broader DSA expert community. Having successfully positioned themselves as experts on DSA compliance, they are well placed to influence how regulators and other stakeholders understand risks, and their expectations of appropriate risk management.[163] Many such companies also have personal and professional links with governments and/or platform companies, which could further strengthen their influence.[164] For example, the founder of moderation software provider Cinder previously worked in counterterrorism at Meta and, before that, for the US military, while executives at the specialist DSA consultancy Tremau have worked on digital policy for the French government,[165] and on the Commission team drafting the DSA.[166]

Existing literature discussing how third-party companies could shape DSA systemic risk management has in particular highlighted the problem of corporate capture, suggesting that these companies will tend to promote risk framings that are favorable to the interests of their principal clients, VLOPs.[167] This certainly seems likely, and examples can already be seen. For example, Tremau has argued in talks aimed at the professional trust and safety community that because risk assessments are very difficult for VLOPs, CSOs should not have overly high expectations and should give the companies 'just a little bit of

---

[160] While the risk management provisions relate exclusively to VLOPs, smaller companies are expected to rely particularly heavily on third-party software and services for other aspects of DSA compliance, such as content moderation: Keller (n 46).

[161] European Commission, 'Digital Services Act: technical assistance for market intelligence, evidence gathering and compliance monitoring' (*EU Funding & Tenders Portal*, 5 August 2024) https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/tender-details/efd2992a-c0a2-498c-83ca-a1729a3863ff-CN accessed 22 January 2025.

[162] Kenneth A Bamberger, 'Technologies of Compliance: Risk and Regulation in a Digital Age' (2010) 88 Texas Law Review 609.

[163] See, eg, the participation by Tremau and Deloitte consultants in a recent event hosted by one of the leading academic experts on the DSA, 'Decoding DSA Risk Assessments and Audits' (LSE *Law School*, 22 January 2025) https://lselaw.events/event/decoding-dsa-risk-assessments-and-audits/ accessed 22 January 2025.

[164] Wei and others (n 64).

[165] Bernard (n 156).

[166] Comments by Martin Husovec in 'Decoding DSA Risk Assessments and Audits' (n 163).

[167] Terzis and others (n 155); Johann Laux, Sandra Wachter and Brent Mittelstadt, 'Taming the Few: Platform Regulation, Independent Audits, and the Risks of Capture Created by the DMA and DSA' (2021) 43 Computer Law & Security Review 105613 https://doi.org/10.1016/j.clsr.2021.105613.

grace'.[168] It has also suggested that VLOPs could leverage risk management processes for commercial benefits, such as improving user experiences.[169]

However, third-party companies also have their own, varying commercial interests. Participation in conferences and other events or talks aimed at the DSA expert community is effectively a marketing strategy, and for obvious reasons, these companies will tend to promote understandings of risk that create a need for their own products and services.[170] For example, software providers may try to frame systemic risks as relatively simple and amenable to technical solutions that can be implemented using off-the-shelf software (for example, suggesting that risks primarily involve harmful content that needs to be identified and removed). In contrast, consultants may prefer to frame risks as demanding more disruptive organizational changes that require expert support.[171] Finally, auditors generally do not want the responsibility for making substantive decisions about how risks should be managed, as this could create liability risks for them.[172] Consequently, they typically push VLOPs to focus on demonstrating appropriate risk management processes, rather than on substantive policy questions.[173]

As this last point illustrates, external professionals can shape the construction of risk not only through explicit advocacy but also more subtly, by validating particular knowledge production and risk management techniques. Power's research on auditing suggests that it pushes companies towards more standardized, formalized processes and quantifiable metrics.[174] Based on interviews with auditors and platform staff, Daphne Keller argues that this tendency is already visible in the DSA context.[175] Importantly, since auditors and third-party providers will often work for multiple VLOPs, their involvement may also encourage industry-wide standardization of risk management approaches.[176]

---

168 Comments by Agne Kaarlep in 'Decoding DSA Risk Assessments and Audits' (n 163).

169 Comments by Agne Kaarlep in 'Risk Assessments with Agne Kaarlep' (*Safety is Sexy Podcast*, 17 September 2024) www.matthewsoeth.com/safety-is-sexy-podcast/risk-assessments-with-agne-kaarlep accessed 23 October 2024.

170 Obendiek and Seidl (n 33).

171 Laleh Khalili, 'In Clover' (*London Review of Books*, 44(24), 15 December 2022) www.lrb.co.uk/the-paper/v44/n24/laleh-khalili/in-clover accessed 22 January 2025.

172 European Contact Group, 'ECG responds to the EC call for feedback on the Digital Services Act audit methodology draft delegated regulation' (4 July 2023) www.europeancontactgroup.eu/news/ecg-responds-to-the-ec-call-for-feedback-on-the-digital-services-act-audit-methodology-draft-delegated-regulation/ accessed 22 January 2025.

173 Keller (n 46).

174 This enables auditors to assure the adequacy or reliability of companies' risk management processes, without explicitly making their own policy judgments about how risks should be managed. That minimizes the 'audit risk' or 'secondary risk' that eventual misconduct by audited companies will be blamed on poor auditing: see Power, 'Risk Management of Nothing' (n 49); Michael Power, *The Audit Society: Rituals of Verification* (OUP 1997).

175 Keller (n 46).

176 Griffin, 'Brand Safety' (n 73); Keller (n 46). See also Bamberger, 'Technologies of Compliance' (n 162).

3.3.2. Non-Governmental Organizations

Advocacy by independent organizations can not only shape how regulators, companies and other elite actors understand and address particular policy issues, but can also 'politicize' and contest problem framings that otherwise enjoy elite consensus.[177] Alongside NGOs, stakeholders can also mobilize around platform governance through more loosely-organized political campaigns,[178] or other civil society organizations such as unions.[179] However, NGOs often have the necessary resources and connections to participate in influential policy circles in ways that other actors cannot – especially in the elite-dominated, technocratic world of EU policymaking.[180]

Unsurprisingly, then, NGOs figure prominently in the DSA expert community, and there is a broad consensus that civil society participation – most often understood as participation by NGOs – is essential in order for systemic risk management to be legitimate and effective.[181] NGOs are understood as providing external accountability for VLOPs and regulators, and as representing the views of users and affected communities.[182] This is in line with longstanding 'best practices' in trust and safety policy,[183] and with established approaches to human rights due diligence, which heavily emphasize consultation with affected stakeholders.[184] In this vein, the DSA includes numerous provisions mandating or encouraging VLOPs and regulators to consult with civil society organizations and involve them in standard-setting.[185] Regulators have also established further processes to solicit civil society input: DG Connect holds private 'roundtable' discussions with selected NGOs,[186] while Germany's Bundesnetzagentur has created a standing advisory committee of selected academic and civil society experts.[187]

---

[177] Liedlbauer (n 142).

[178] See, eg, everybodyvisible, 'ANNOUNCING our EveryBODYVisible campaign and day of action on 29 October 2019' (*Instagram*, 12 October 2019) www.instagram.com/everybodyvisible/p/B3hegPcpz33/?img_index=1 accessed 22 January 2025.

[179] See, eg, Njenga Kimani and others, 'Checking on the Progress of Content Moderators in Africa' (Tech Policy Press, 3 December 2023) www.techpolicy.press/checking-on-the-progress-of-content-moderators-in-africa/ accessed 22 January 2025.

[180] Reem Ahmed, 'Negotiating Fundamental Rights: Civil Society and the EU Regulation on Addressing the Dissemination of Terrorist Content Online' (2023) Studies in Conflict & Terrorism https://doi.org/10.1080/1057610X.2023.2222890.

[181] Niklas Eder, 'Making Systemic Risk Assessments Work: How the DSA Creates a Virtuous Loop to Address the Societal Harms of Content Moderation' (2024) 25(7) German Law Journal 1197 https://doi.org/10.1017/glj.2024.24.

[182] DSA Decoded (n 12); Global Network Initiative & Digital Trust & Safety Partnership (n 124).

[183] Dvoskin (n 36).

[184] Duval (n 154).

[185] See, eg, Recital 90 on VLOPs' risk assessment processes, Article 62(5) and (6) on the Board, and Articles 45(2), 46(1) and 47(1) on civil society participation in drafting codes of conduct; for a more comprehensive overview of relevant provisions, see Carvalho (n 28).

[186] European Commission, 'Second online roundtable with Civil Society Organizations on the implementation of the Digital Services Act' (9 July 2024) https://digital-strategy.ec.europa.eu/en/news/second-online-roundtable-civil-society-organizations-implementation-digital-services-act accessed 22 January 2025.

[187] Bundenetzagentur, 'Erste Sitzung des Beirates des Digital Services Coordinators bei der Bundesnetzagentur' (18 September 2024) www.bundesnetzagentur.de/10284772 accessed 22 January 2025.

Beyond these formal participation mechanisms, NGOs can shape risk management in various other ways. As discussed in section 3.2.3, strategic litigation could be one important way of contesting dominant approaches to risk management. This could involve bringing lawsuits or intervening directly in legal proceedings;[188] strategically supporting individual litigation by individuals (which is already happening in national-level cases involving the DSA[189]); or, potentially, bringing representative claims on behalf of larger classes.[190] Litigation could clarify contested questions around DSA interpretation, but importantly, its impacts can also go beyond the direct legal outcome, as part of a broader strategy to politicize issues, initiate public debates and attract support.[191]

Research and independent expertise have also historically been important areas for digital rights NGOs, and in the DSA systemic risk framework, the production of knowledge and expertise about risks is already emerging as a key area of political contestation. NGOs have leveraged the demand for authoritative methodologies, metrics and best practices in order to advocate for their own political agendas – both by promoting specific risk management approaches and methods, and by drawing attention to particular topics.[192] The DSA's data access provisions, which can also be used by NGOs,[193] could also make it easier for them to shape policy debates through research and advocacy.

Thus far, the most prominent organizations operating in this space have been digital rights NGOs specializing in technology regulation, such as the Center for Democracy and Technology (CDT), Access Now and AlgorithmWatch, as

---

188 Valentina Golunova and Mariolina Eliantonio, 'Civil Society Actors as Enforcers of the GDPR: What Role for the CJEU?' (2024) 15 JIPITEC 180.

189 See Bering and Vezzoso (n 140).

190 This is possible under the EU's 2020 Representative Actions Directive: see Digital Freedom Fund, 'Intersection with the Digital Services Package and other EU Regulatory Instruments' (Collective Redress: Lessons from Around the Globe, 13 December 2020) https://digitalfreedomfund.org/collective-redress-lessons-from-around-the-globe/ accessed 22 January 2025. The Dutch NGO SOMI has already filed representative actions on behalf of consumers in the Netherlands, Germany and Belgium against TikTok, Meta and X: Stichting Onderzoek Marktinformatie, 'All cases' https://somi.nl/en/all-cases accessed 8 May 2025.

191 Liedlbauer (n 142).

192 See, eg, Anna-Katharina Meßmer and Martin Degeling, 'Auditing Recommender Systems: Putting the DSA into practice with a risk-scenario-based approach' (*Interface*, 7 February 2023) www.interface-eu.org/publications/auditing-recommender-systems accessed 23 January 2025; Katarzyna Szymielewicz and others, 'Safe By Default' (*Panoptykon*, March 2024) https://panoptykon.org/sites/default/files/2024-03/panoptykon_peoplevsbigtech_safe-by-default_briefing_03032024.pdf accessed 23 January 2025; Oliver Marsh, 'Researching Systemic Risks under the Digital Services Act' (*AlgorithmWatch*, 21 August 2024) https://algorithmwatch.org/en/researching-systemic-risks-under-the-digital-services-act/ accessed 23 January 2025.

193 NGOs can access public databases and APIs that VLOPs are required to establish under Articles 24(5), 39 and 40(12). NGO staff could also in some circumstances be certified as vetted researchers and access VLOPs' internal data under Article 40(4) (if they qualify as a 'research organization' under Article 40(8)), and could also commission or collaborate on academic research: see Julian Jaursch and Philipp Lorenz-Spreen, 'Researcher Access to Platform Data Under the DSA: Questions and Answers' (*Interface*, 2023) www.interface-eu.org/publications/researcher-access-platform-data-under-dsa-questions-and-answers accessed 23 January 2025. The extent to which non-academic researchers will be able to utilize Article 40(4) has been a prominent topic in expert discussions around the data access framework – illustrating the strategic importance that NGOs in this field attach to research and knowledge production.

well as EDRi, which represents a network of NGOs focusing on digital rights. These specialized organizations have not only built up relevant expertise and resources, but also developed close connections with policymakers, academics and platform companies. However, NGOs in other fields have featured prominently in discussions around certain aspects of risk management, such as child safety.[194] In future, NGOs involved in other aspects of DSA enforcement – for example, as certified dispute resolution institutions for content moderation[195] or 'trusted flaggers' of illegal content[196] – might be able to effectively position themselves as experts on particular risk areas.[197]

How might NGOs shape the politics of DSA systemic risks? In academic research and expert discussions, 'stakeholder engagement' is often discussed as a way to democratize platform governance and give affected communities, especially minoritized or vulnerable groups, a voice in regulatory regimes.[198] NGOs are seen simultaneously as sources of independent expertise, capable of advocating for the 'public interest' where it conflicts with the interests of governments and/or corporations, and as representing the perspectives and 'lived experiences' of particular interest groups and communities affected by platform governance.[199] As Caroline Lee, Kelly McNulty and Sarah Shapper argue, this conception of 'civil society' does important discursive work in regulatory politics.[200] Emphasizing the idea of political actors motivated by abstract conceptions of the public interest, independent from state or commercial interests, can disguise and defuse political conflicts – framing them in terms of cooperative, deliberative processes, rather than as power struggles between actors with conflicting interests and very unequal material resources.[201]

---

[194] For example, the committee appointed by the Commission to draft a code of conduct on risks to minor safety includes representatives from three organizations that focus on child abuse and exploitation, and two that focus on children's rights and welfare in general: European Commission, 'Special group on the EU Code of conduct on age-appropriate design' (20 September 2023) https://digital-strategy.ec.europa.eu/en/policies/group-age-appropriate-design accessed 23 January 2025.

[195] See Art 21, DSA (n 1).

[196] See Art 22, DSA (n 1).

[197] These institutions are at a relatively early stage of development and few organizations have so far been certified, so which particular organizations and perspectives will be represented remains an open question.

[198] Dvoskin (n 36).

[199] Carvalho (n 28).

[200] Lee and others, 'Civic-izing Markets' (n 42); see also Edward T Walker, 'Legitimating the Corporation Through Public Participation' in Caroline W Lee, Michael McQuarrie and Edward T Walker (eds), *Democratizing Inequalities: Dilemmas of the New Public Participation* (NYU Press 2015).

[201] See also Juanita Uribe, 'Excluding Through Inclusion: Managerial Practices in the Era of Multistakeholder governance' (2024) 31 Review of International Political Economy 1686 https://doi.org/10.1080/09692290.2024.2362666.

Yet self-evidently, the European civil society landscape is anything but free of state and corporate influence. NGOs often depend directly for funding on state actors, VLOPs and other corporations, and/or philanthropic foundations which typically have corporate connections.[202] Their participation can also be influenced in more subtle ways. Corporate experts can effectively manage participatory processes in order to legitimize their own business practices and defuse opposition.[203] For example, in DSA risk assessments, VLOPs will inevitably exercise significant influence over the procedures and outcomes of any consultation process – not only by selectively granting access and deciding which participants to listen to, but also by deciding which 'risks' to consult on, and how questions about these risks are framed.[204]

More generally, NGOs are far from representative of any generalized public interest. The organizational capacities and financial resources necessary to use the various channels for participation discussed in this section – attending expert events and discussions; participating in consultations and gaining informal access to VLOPs and policymakers; producing and commissioning research; bringing or supporting lawsuits – are very unequally distributed.[205] Relying on NGOs as representatives of the public privileges a particular form of elite-driven political participation, sidelining other forms of public political mobilization, such as trade unions.[206] It also typically leads to the overrepresentation of wealthier and more powerful interests[207] – or forms of contestation that are acceptable, even if not actually favorable, to those interests.[208]

These unequal capacities are certainly visible in relation to the DSA. Events and policy discussions not only tend to overrepresent a relatively small group of specialist digital rights organizations; they are also dominated by organizations based in wealthier northern and western European member states.[209] In theory, given the broad scope of Articles 34–35, participation should not require specialist digital policy expertise, and could involve a very broad range

---

[202] Jake Goldenfein and Monique Mann, 'Tech Money in Civil Society: Whose Interests Do Digital Rights Organizations Represent?' 37(1) Cultural Studies 88 https://doi.org/10.1080/09502386.2022.2042582; Eugenia Siapera and Elizabeth Ferries, 'Platform Governance and Civil Society Organisations: Tensions Between Reform and Revolution Continuum' (2025) 14(1) Internet Policy Review https://doi.org/10.14763/2025.1.2002.

[203] Lee and others, 'Civic-izing Markets' (n 42); Walker (n 200); Edward T Walker, Michael McQuarrie and Caroline W Lee, 'Rising Participation and Declining Democracy' in Caroline W Lee, Michael McQuarrie and Edward T Walker (eds), *Democratizing Inequalities: Dilemmas of the New Public Participation* (NYU Press 2015).

[204] Dvoskin (n 36); Walker (n 200).

[205] Griffin, 'Public and Private Power' (n 35); Siapera and Ferries (n 202).

[206] Walker (n 200); Siapera and Ferries (n 202). Unions and workers' rights are conspicuously absent from the DSA, even though content moderation and platform governance raise widely-recognized labor rights issues.

[207] Walker (n 200); Kampourakis (n 53).

[208] Griffin, 'Public and Private Power' (n 35); Michael Kwet, *Digital Degrowth: Technology in the Age of Survival* (Pluto 2024), ch 9.

[209] Orlando-Salling (n 132).

of organizations.[210] In practice, however, organizations representing particularly marginalized and vulnerable social groups are more likely to face barriers related to limited funding and capacities. Finally, these disparities affect not only who has access to expert spaces, but also who is listened to within these spaces. For example, the importance attached to legal and technical expertise may make it harder for groups who cannot afford to hire professional experts to present their views in a form likely to be taken seriously by VLOPs and regulators. NGOs may also find that in order to be seen as serious experts, they have to respond to narrowly-framed questions or present their input in terms of technical expertise that can inform commercial decisions, rather than explicitly challenging VLOPs' normative choices and business strategies.[211] In these ways, the importance attached to expertise in risk management can effectively serve to reinforce power disparities in platform governance and marginalize the perspectives of disadvantaged groups, even in processes that are seemingly designed to enable participation by diverse stakeholders.

3.3.3. Academic Researchers and Institutions

As well as industry-specific expertise, risk regulation generally creates a strong demand for scientific advice – which is seen as both independent and authoritative.[212] This is especially so in technically complex fields, even though such fields are often also characterized by scientific uncertainty and disagreement (which is the case in many areas relevant to DSA systemic risks, as noted in the introduction). Consequently, perhaps even more than NGOs, academics play an essential role in informing risk management and validating particular understandings of risk,[213] as well as – sometimes – critiquing and contesting other actors' understandings of risk.[214]

EU and national regulators have stated that academic research will play an essential role in both informing and scrutinizing DSA enforcement.[215] EU and national-level regulatory agencies have established research institutions and advisory bodies,[216] while VLOPs' consultation processes have historically included

---

[210] Carvalho (n 28).

[211] Siapera and Ferries (n 202).

[212] Ulrich Beck, *Risk Society: Towards a New Modernity* (Mark Ritter tr, Sage Publications 1992).

[213] Beck, *Risk Society* (n 212).

[214] Ahmed (n 180).

[215] DSA Decoded (n 12).

[216] At the EU level, a prominent example is the European Centre for Algorithmic Transparency and European Digital Media Observatory. At the national level, Germany's Bundesnetzagentur has an advisory council of academic and civil society experts, while France's Arcom holds an annual 'research day' for academics to present on relevant topics: Julian Jaursch, 'Der Beirat beim deutschen DSC: Über- und Ausblick' (*Interface*, 17 April 2024) www. interface-eu.org/publications/advisory-body-german-dsc-overview-and-open-questions-1 accessed 27 January 2025; Arcom, 'Appel à contribution : troisième journée d'études de l'Arcom' (23 May 2024) www.arcom.fr/espace-professionnel/consultations-publiques-et-etudes-dimpact/appel-contribution-troisieme-journee-detudes-de-larcom accessed 27 January 2025.

academic experts.[217] As discussed above, several DSA provisions (notably Article 40(4) on access to internal data, Article 40(12) on access to public data and Articles 24(5) and 39 on public archives) aim to enable more academic research into platforms, based on the assumption that knowing more about platforms and their social impacts is a precondition for more effective governance.[218]

Notwithstanding this consensus, questions can be raised about how influential academics will be in practice, and how far demands for independent expertise can actually be met. While better data access will in time undoubtedly facilitate more independent research into platform governance,[219] so far researchers have run into numerous practical issues. Questions have been raised about the accuracy and consistency of VLOPs' public databases and transparency reports.[220] Some Article 40 requests have been rejected, or responded to with unreliable or incomplete data.[221] These processes may become more streamlined and reliable over time. Even so, there are inherent limitations on the validity and generalizability of research based on internal data produced for commercial purposes, from platforms whose technical interfaces and design features change regularly.[222]

More fundamentally, even with more and better research being produced, its influence should not be overestimated. Mainstream discourse about academic research in platform governance often seems to be based on a depoliticized understanding of regulation, assuming that addressing difficult policy issues simply requires knowing more about them – implicitly, because this will indicate objectively better solutions – as opposed to making contestable distributive and ideological choices. Scholarship on risk regulation in other fields suggests that academic research can indeed be influential, but less because it inherently points to the right policy choices, and more because of how it is strategically mobilized by political actors.[223] In the DSA context, while regulators repeatedly emphasize the essential role of academic research in inform-

---

217 Dvoskin (n 36).

218 Leerssen, 'Black Box' (n 27).

219 For some early examples, see Charis Papaevangelou and Fabio Votta, 'Content Moderation and Platform Observability in the Digital Services Act' (*Tech Policy Press*, 29 May 2024) www.techpolicy.press/content-moderation-and-platform-observability-in-the-digital-services-act/ accessed 23 January 2025; Rishabh Kaushal and others, 'Automated Transparency: A Legal and Empirical Analysis of the Digital Services Act Transparency Database' (2024) arXiv https://doi.org/10.48550/arXiv.2404.02894.

220 Amaury Trujillo, Tiziano Fagni and Stefano Cresci, 'The DSA Transparency Database: Auditing Self-reported Moderation Actions by Social Media' (2024) arXiv https://arxiv.org/pdf/2312.10269 accessed 23 January 2025.

221 Philipp Darius, 'Researcher Data Access Under the DSA: Lessons from TikTok's API Issues During the 2024 European Elections' (*Tech Policy Press*, 24 September 2024) www.techpolicy.press/-researcher-data-access-under-the-dsa-lessons-from-tiktoks-api-issues-during-the-2024-european-elections/ accessed 23 January 2025; DSA 40 Collaboratory, 'Tracker Insights' (8 January 2025) https://dsa40collaboratory.eu/tracker-insights/ accessed 23 January 2025.

222 Kevin Munger, 'Is The Best Social Science Good Enough?' (*Never Met a Science*, 10 July 2024) https:// kevinmunger.substack.com/p/is-the-best-social-science-good-enough accessed 23 January 2025.

223 Adekola (n 16); Boyd (n 37).

ing and scrutinizing risk management, it could be questioned how much it will actually substantively influence their policy choices – or indeed, whether invoking academic expertise simply serves as a way for regulators to authorize and depoliticize their own decisions.

Finally, the idea of academia as a space for disinterested knowledge production, guided only by the public interest, should also be problematized. A long tradition of scholarship in science and technology studies (STS) has explored how institutional norms, ideologies and power dynamics shape the construction of scientific knowledge; this extensive literature cannot be fully reviewed here, but has fairly conclusively dismissed any idea that scientific knowledge can be objective or apolitical.[224] More practically, academia is a sphere with its own norms, established practices and institutional incentives, which do not necessarily align with the goals of informing regulatory enforcement or preventing harmful business activities.[225] The research questions which researchers and journals find interesting, and which can attract institutional resources and grant funding, may not necessarily provide the evidence that VLOPs and regulators are looking for.

Finally, the political economy of academic knowledge production could also reinforce existing inequalities in risk politics. Academic research will tend to overrepresent issues relevant to the larger and wealthier EU member states, which have better-resourced university systems.[226] Reliance on private grant funding and data access also creates possibilities for corporate capture, similar to those discussed above in relation to NGOs.[227] Importantly, this does not require unethical behavior by individual academics or institutions; companies can selectively fund research topics and critical approaches that are less threat-

---

[224] Wynne (n 39).

[225] Importantly, this is generally considered a good thing, preserving the autonomy of academic institutions as a space for relatively independent intellectual exploration: Wendy Brown & Daniel Steinmetz-Jenkins, 'Wendy Brown: A Conversation on Our "Nihilistic" Age' (*The Nation*, 10 January 2024) www.thenation.com/article/culture/wendy-brown-interview/ accessed 23 January 2025. Attempts to make academic research more reflective of regulatory priorities, such as the provisions in Articles 40(4) and 40(12) DSA that research data access should be permitted only where it contributes to the understanding of systemic risks, have justifiably been criticized for compromising academic independence: Martin Fertmann and Tobias Mast, 'Forschungsdatenzugang und Technologieregulierung' (2024) 57(2) Wissenschaftsrecht 101 https://doi.org/10.1628/wissr-2024-0011.

[226] Benedetto Lepori, Daniel Wagner-Schuster and Marija Breitfuss-Loidl, *How are European Higher Education Institutions Funded? New Evidence from ETER Microdata* (European Tertiary Education Register, 2019) https://eter-project.com/uploads/analytical-reports/ETER_AnalyticalReport_02_final.pdf accessed 23 January 2025; Balázs Bodó, Dániel Antal and Zoltán Puha, 'Can Scholarly Pirate Libraries Bridge the Knowledge Access Gap? An Empirical Study on the Structural Conditions of Book Piracy in Global and European Academia' (2020) 15(12) PLOS One https://doi.org/10.1371/journal.pone.0242509.

[227] Wei and others (n 64); Jefferson Pooley, 'Data Dependencies and Funding Prospects: A 1930s Cautionary Tale' (2021) 2(2) Harvard Kennedy School Misinformation Review; David Gray Widder, Meredith Whittaker and Sarah Myers West, 'Why "Open" AI Systems are Actually Closed, and Why This Matters' (2024) 635 Nature 827 https://doi.org/10.1038/s41586-024-08141-1.

ening to their business interests.[228] Finally, because scientific evidence and expertise plays such a significant role in producing and authorizing knowledge about risks, political claims may effectively need to be validated through academic research in order to be taken seriously by experts.[229] This privileging of elite technocratic knowledge can effectively function to close off more broad-based public contestation of risk.[230]

3.3.4. Media

Finally, although they are not directly involved in DSA enforcement in the same way as the other stakeholders discussed here, the role of media organizations and journalists should not be overlooked. Scholarship on the social amplification of risk – which originally drew inspiration from communications science – emphasizes the role of the media in shaping public and elite perceptions of risks, and thereby amplifying or attenuating their effects.[231] Similarly, in political science and regulatory politics, news media are generally understood to play an important role in framing policy issues and setting political agendas.[232]

Platform regulation is no exception. Large news publishers and other major media corporations have been influential lobby groups in specific regulatory debates affecting their own interests, such as the moderation of copyright-infringing content.[233] These well-connected corporate actors could also influence how policymakers and regulators construct systemic risks, both through direct political lobbying, and by producing knowledge and mobilizing expertise. For example, copyright industry groups have already been certified as trusted flaggers,[234] which could help them position themselves as experts on the moderation of illegal content, in a similar way to law enforcement agencies (as discussed in section 3.2.4).

---

[228] Wei and others (n 64); Kwet (n 208); Laurie Clarke, Oscar Williams & Katherine Swindells, 'How Google quietly funds Europe's leading tech policy institutes' (*New Statesman*, 30 July 2021) www.newstatesman.com/science-tech/2021/07/how-google-quietly-funds-europe-s-leading-tech-policy-institutes accessed 23 January 2025.

[229] Beck, *Risk Society* (n 212).

[230] Wynne (n 39).

[231] Kasperson and others (n 10); Adekola (n 16).

[232] Peter Van Aelst and Stefaan Walgrave, 'Political Agenda Setting by the Mass Media: Ten Years of Research, 2005–2015' in Nikolaos Zahariadis (ed), *Handbook of Public Policy Agenda Setting* (Elgar 2016).

[233] Annemarie Bridy, 'The Price of Closing the Value Gap: How the Music Industry Hacked EU Copyright Reform' (2020) 22 Vanderbilt Journal of Entertainment & Technology Law 323; Terry Flew and others, 'Return of the Regulatory State: A Stakeholder Analysis of Australia's Digital Platforms Inquiry and Online News Policy' (2021) 37 The Information Society 128, 129 https://doi.org/10.1080/01972243.2020.1870597.

[234] European Commission, 'Trusted flaggers under the Digital Services Act (DSA)' (28 March 2025) https://digital-strategy.ec.europa.eu/en/policies/trusted-flaggers-under-dsa accessed 1 April 2025; and see generally Naomi Appelman and Paddy Leerssen, 'On "Trusted' Flaggers"' (2022) 24 Yale Journal of Law & Technology 541.

Moreover, media organizations do not only exert influence in favor of their own direct interests; they also play an important role in amplifying the influence of other stakeholders, for example by drawing attention to civil society campaigns. Politicians and regulators may generally promote risk framings likely to attract favorable media coverage. For example, this may be one factor behind the Commission's growing focus on child safety, an issue which consistently attracts media attention.[235] Similarly, because reputational pressure from the media shapes public perceptions and regulators' priorities, how VLOPs approach DSA compliance is likely to be influenced by the possibility of positive or negative media coverage.[236]

4 Concluding Thoughts and Research Agenda

The DSA systemic risk framework represents a major development in the regulation of platforms with millions or billions of users, which are owned and operated by some of the world's largest and most powerful companies, and which now intermediate large portions of many societies' media consumption, cultural production, social interaction and political discourse. The implementation of this regulatory framework thus represents an important terrain for political contestation over how these influential platforms should be governed.

This article has presented a first attempt to map out this political landscape, showing that systemic risk management will be shaped by diverse private and public stakeholders, with different political priorities and material interests, as well as their own internal conflicts. How VLOPs approach systemic risk management will ultimately depend on how these actors compete and collaborate to build or challenge shared understandings about the definition, understanding, prioritization and mitigation of risk. Because of the value attached to specialized expertise in digital governance and the technical nature of corporate risk management processes, these negotiations will largely take place within the expert community that has already coalesced around the DSA and its implementation. The DSA also provides important opportunities for external stakeholders to contest expert consensus, as some civil society actors are already actively doing. Yet these external stakeholders' interests and resources reflect pre-existing power dynamics and inequalities, and may also be vulnerable to capture by state or corporate interests. Ultimately, given these unequal capacities, and the dominance of technical experts and industry perspectives in the DSA expert community, it is doubtful whether the systemic risk framework will allow much

---

[235] Amy Orben, 'The Sisyphean Cycle of Technology Panics' (2020) 15 Perspectives on Psychological Science 1143 https://doi.org/10.1177/1745691620919372.

[236] Marchal and others (n 72).

input from particularly marginalized communities, or genuinely radical perspectives about how platform governance might be reformed.

That said, with DSA implementation still in its early stages, these can only be preliminary conclusions. Which actors will most successfully shape expert discussions around systemic risk management, which understandings of risk will gain currency, and how they will concretely impact VLOPs' business practices are very much still open questions. To a large extent, they are empirical questions; the analysis presented in this article should thus be considered as presenting hypotheses that require further investigation. As more information becomes available about how VLOPs, regulators and other stakeholders are approaching risk management, future research should build on this mapping of the stakeholder landscape by investigating and critically analyzing the political agendas and priorities of the different actors and stakeholder groups; the strategies they use to advocate for these agendas; and the relative influence of different stakeholders, agendas and strategies. This article thus concludes with some thoughts on the most important directions for future research.

First, in relation to VLOPs, research could investigate their published risk assessment reports and other statements, using methods such as content analysis and critical discourse analysis to investigate which issues are being identified as risks, how they are framed, and how they are being mitigated. This should include descriptive research (for example, identifying industry-wide trends) as well as more critical or normative analyses of their political priorities and problem framings. Research could also investigate VLOPs' actual risk management processes, asking questions about how responsibility is allocated between teams, what kinds of problems and solutions are considered, and which make it into the final assessment. While these processes will inevitably be somewhat opaque, sociolegal research has successfully shed light on tech companies' decision-making procedures, based on negotiated access and/or other approaches, such as interviewing current and former employees, or attending industry events and conferences.[237] Relatedly, studying the professional trust and safety community could not only offer insights into VLOPs' practices, but also in itself presents important research questions. For example, to what extent are trust and safety professionals recognized as experts by other actors (such as academic and government institutions), and is the professionalization of trust and safety promoting industry-wide standardization of risk management?

With regard to state agencies, research could use public statements, interviews, and other sources (such as freedom of information requests for internal documents[238]) to investigate and critically analyze the enforcement strategies and political agenda(s) of the Commission and other relevant agencies. Similarly, as more court rulings involving the DSA emerge, there will be plenty of scope for

[237] See, eg, Klonick, 'New Governors' (n 54); Waldman, *Industry Unbound* (n 84).

[238] See, eg, Gorwa, *Politics of Platform Regulation* (n 55).

legal research exploring their implications for the understanding and management of systemic risks, as well as clarifying jurisdictional and doctrinal questions. In addition, research should critically analyze the political implications of regulatory and judicial decisions. This could also involve situating DSA enforcement in relation to European policymakers' wider political agendas: for example, how practically significant is the reframing in Virkkunen's portfolio of platform regulation as an issue of European sovereignty and security? [239]

The four broad categories of external stakeholders identified here also raise many important questions. Future descriptive research could better develop our understanding of the stakeholder landscape by more systematically investigating and documenting which actors are participating in DSA risk management: for example, what companies are offering compliance-related services, [240] which NGOs are working on DSA systemic risks, and what are their favored understandings of risk? Research could also investigate which understandings of risk are being promoted most successfully, and which advocacy strategies are most effective, as well as which fora or 'loci of participation' external stakeholders find most advantageous. [241] It could also illuminate how disparities of economic resources and political connections affect these forms of participation. For example, which external stakeholders are getting access to (private or public) consultations with VLOPs and regulators; which actors are able to bring questions about DSA interpretation to court; and which legal arguments are successful? Finally, research could investigate not only how systemic risks are framed and understood within academic research and popular media – and how resource disparities shape the attention allocated to different areas – but also which scientific framings and evidence are adopted and mobilized by VLOPs, regulators and other political actors.

As these last points suggest, mapping and categorizing stakeholder groups is only a starting point. A crucial element of risk politics is the relationships and interactions between stakeholders, which represent a key source of political power. [242] A major factor reinforcing power imbalances in risk regulation is that large companies and other wealthy and/or elite groups tend to have privileged connections with other influential stakeholders – as illustrated by the growing body of research documenting 'big tech' companies' enormous lobbying spending [243] and their close relationships with academic institu-

---

239 European Commission, 'Commissioners-designate' (n 127).

240 For a recent example of such work see Sipos (n 158).

241 Carvalho (n 28).

242 Adekola (n 16).

243 Corporate Europe, 'Lobbying in Times of Trilogues' (n 103); Corporate Europe, 'Byte by Byte' (n 103); Corporate Europe, 'Big Tech Lobby Power in Brussels Continues to Grow' (*Corporate Europe*, 7 September 2023) https://corporateeurope.org/en/2023/09/big-tech-lobby-power-brussels-continues-grow accessed 25 December 2024.

tions[244] and media publishers.[245] Conversely, building relationships with more powerful stakeholders can also enable less powerful stakeholder groups and minority perspectives to influence risk politics. As indicated in section 3, the DSA offers some significant openings for less powerful stakeholders to contest dominant understandings of risk through tactics such as strategic litigation, media campaigns and the mobilization of scientific research[246] – but there is also ample scope for 'independent' expertise and multistakeholder participation to be co-opted by powerful state and corporate interests. Tracing how risks are constructed and contested in practice calls for research that does not only analyze stakeholder groups in isolation, but explores ongoing, dynamic interactions and relationships between stakeholders, in order to understand how coalitions build consensus around particular understandings of risk, and how dominant understandings may be destabilized.

Acknowledgements

Thank you to Paddy Leerssen and Riccardo Fornasari for many thought-provoking discussions on the political economy of platform regulation and the politics of risk, and to Claire Stravato Emes and Mateus Correia de Carvalho for their invaluable comments on earlier drafts.

Date received: January 2025
Date accepted: April 2025

[244] Widder and others (n 227); Kwet (n 208).

[245] Charis Papaevangelou and Nikos Smyrnaios, 'The Political Stakes of Online Platforms' Deals with French Publishers' (2023) 68 Anàlisi: Quaderns de Comunicació i Cultura 177.

[246] Birkland (n 17).