GENEVA ACADEMY
Académie de droit international humanitaire et de droits humains
Academy of International Humanitarian Law and Human Rights

RESEARCH BRIEF

EUROPEAN UNION DATA ACCESS FOR STUDY OF DIGITAL DISINFORMATION OPERATIONS

ABSTRACT

The European Union's regulatory approach to researcher access under the Digital Services Act marks a significant step forward in the fight against digital disinformation operations (disinfo-ops). As so-called 'synthetic forces' exploit online platforms with minimal transparency, structured access to platform data is essential for understanding systemic risks, algorithmic amplification of false content, and the broader impact on governance processes. This Info-Brief examines how the EU's legal framework facilitates independent research while balancing privacy and security concerns. By mandating data access for vetted researchers, the suite of legislative initiatives sets a global precedent for external scientific study.

MARCH 2025 | STEVEN J. BARELA

This publication has been externally peer-reviewed

THE GENEVA ACADEMY A JOINT CENTER OF
GENEVA GRADUATE INSTITUTE
INSTITUT DE HAUTES ÉTUDES INTERNATIONALES ET DU DÉVELOPPEMENT
GRADUATE INSTITUTE OF INTERNATIONAL AND DEVELOPMENT STUDIES
UNIVERSITÉ DE GENÈVE
FACULTY OF LAW

INTRODUCTION

Building on the first two reports in this series, this info-brief explores complementary measures to mitigate the impact of mis- and disinformation. A key principle underpinning this work is that any response must align with international law and human rights obligations, empowering individuals while safeguarding fundamental freedoms. Curbing synthetic forces online is a critical step to doing so.[1] This report builds on the legal gaps identified in Part II by spotlighting a pathway to countering disinformation within the multiple international legal frameworks at stake, including defining coercion, reinforcing self-determination conditions, and enhancing empirical foundations for legal accountability.

A core challenge in confronting digital disinfo-ops is the lack of transparency in online ecosystems, where false or misleading content spreads without full understanding. Without structured privacy-preserving access to data, independent researchers lack the ability to measure the scale and precision of these threats or assess the effectiveness of regulatory interventions. In turn, officials lack basic information when it comes to the quantifiable aspects of disinfo-ops, problematizing their ability to set measurable and verifiable limits. This report spotlights an avenue for gathering the needed understanding, replacing uncertainty with empirical clarity and ensuring that policymakers no longer have to navigate this challenge blindfolded.

DATA ACCESS FOR INDEPENDENT RESEARCH

Researcher access to platform data is vital for understanding the risks associated with digital services, including the spread of disinformation, harm to democratic processes, and threats to fundamental rights. In response to these serious challenges, the European Union (EU) has developed a suite of legislative initiatives to enable researcher access to valuable data for scientific study while balancing privacy protection. This includes the General Data Protection Regulation (GDPR) for privacy compliance,[2] the voluntary Code of Practice on Disinformation,[3] and the mandatory obligations set forth under the Digital Services Act (DSA).[4] Together, these frameworks create a robust foundation for increasing transparency and accountability, potentially serving as a global model for data-sharing practices. Moreover, while these regulations apply only to platforms operating within the EU, their implementation can drive broader platform reforms, as companies adjust policies to maintain compliance across multiple jurisdictions.

GDPR & THE CODE OF PRACTICE ON DISINFORMATION

To understand this opening, one begins with the GDPR. This legislation establishes stringent rules for processing personal data, aiming to safeguard individuals' privacy rights in all contexts.[5] Under this law, data access for researchers must comply with key principles such as purpose limitation, data minimization, and security. In other words, the GDPR mandates that personal data be collected and safely processed for clearly defined purposes. In the context of researcher access, it must be demonstrated that the data requested is necessary and proportionate to the objectives of the proposed study. This ensures that only data directly relevant to systemic risks – such as disinformation or platform-driven societal harms – is shared. Data minimization further restricts access to the least amount of data required, reducing potential breaches of privacy.[6] Finally, those who are granted access must demonstrate the technical capacity to safeguard the data from unauthorized exposure.

To protect individual rights, GDPR-compliant measures include anonymization and pseudonymization of data before sharing it with researchers. Platforms are required to implement technical and organizational safeguards, such as encryption and secure storage, to prevent unauthorized access. Researchers, in turn, must adhere to stringent data protection protocols to maintain confidentiality and

integrity throughout their investigations. The integration of GDPR compliance in researcher access frameworks not only protects individuals but also fosters trust among stakeholders, making data-sharing initiatives more sustainable.[7]

While the GDPR safeguards privacy, the EU's Code of Practice on Disinformation serves as a semi-voluntary framework to encourage platforms to share data proactively. This code, tied closely to the Digital Services Act, creates incentives for platforms like Meta, Google, and TikTok to grant researchers access to critical datasets. The Code of Practice emphasizes the sharing of public and non-personal data, such as aggregate statistics or anonymized trends, enabling researchers to analyze patterns without infringing on individual privacy.[8] This allows for the study of disinfo-ops, the spread of harmful narratives, and the impact of algorithmic curation without handling personal user data. Platforms committed to the Code of Practice are encouraged to provide near real-time access to data related to disinformation. This timely access is essential for researchers to track the rapid spread of harmful content and assess the effectiveness of countermeasures. For example, during election cycles or public health crises, real-time data sharing can enable swift action against false narratives.[9]

MANDATING DATA ACCESS: ARTICLE 40 OF THE DSA

The DSA, passed in 2022, represents a landmark shift in the EU's regulatory approach, introducing legally binding obligations for platforms to share data with vetted researchers. Article 40 of the DSA codifies this obligation, establishing a structured process for researcher access and ensuring compliance through regulatory oversight. Under this provision, platforms must grant access to researchers who meet specific criteria, including demonstrating independence, data security competence, and a legitimate research purpose.[10] The vetting process involves national and EU-level regulators, ensuring that only qualified researchers are granted access. This multilayered oversight bolsters the credibility of the data-sharing process while addressing concerns about misuse.

Platforms are required to provide data that enables researchers to investigate "systemic risks", such as disinformation, algorithmic amplification of harmful content, and the erosion of democratic discourse. The law does not provide a general definition of systemic risks, but instead outlines specific categories of risks: dissemination of illegal content, negative effects on certain fundamental rights (privacy, freedom of expression, prohibition on discrimination and the rights of a child), and intentional manipulation of the services.[11] This focus on systemic risks reflects the DSA's broader mandate to ensure that very large online platforms (VLOPs) and very large online search engines (VLOSEs) operate responsibly. Article 40 also includes mechanisms for transparency, requiring platforms to document and justify decisions regarding data access. Researchers, in turn, must publish findings to ensure public accountability and inform policy development. This mutual transparency creates a feedback loop that is meant to enhance the effectiveness of systemic risk mitigation measures.

While Article 40 is a significant step forward, challenges remain in balancing regulatory oversight with the need for flexibility. The complexity of coordinating among national and EU-level regulators and the administrative burden on platforms has slowed implementation (see Delegated Act below). However, by integrating GDPR principles and leveraging insights from the Code of Practice, the DSA provides a solid foundation for advancing data transparency and accountability.

THE DRAFT DELEGATED ACT

On 29 October 2024, five months after a call for evidence was closed, the European Commission published a draft Delegated Act for Data Access under Article 40 of the DSA which outlines the technical mechanisms to facilitate researcher access to data from VLOPs and VLSOEs.[12] The draft was open for public consultation and feedback for six weeks, and the Commission plans to adopt the rules in the second quarter of 2025.

An essential element of the draft Delegated Act is the creation of the DSA Data Access Portal, designed as a streamlined "one-stop shop" for researchers, regulators, and platforms. The portal ensures procedural consistency across member States while offering a public overview of successful "reasoned requests." This transparency allows researchers to learn from past applications and develop robust proposals.[13] However, data transmission remains decentralized, conducted through secure environments managed by platforms or certified third parties. The proposal emphasizes flexibility in access modalities, including options for secure interfaces and data storage.

Of note, the Delegated Act also introduces a mandatory requirement for these platforms to create a "data inventory," detailing the datasets available for research and their

respective access modalities. This inventory, acting as a comprehensive "codebook," addresses a common barrier in research – the uncertainty about what data is available to be accessed. As such, researchers can focus their proposals on existing data while acknowledging the dynamic nature of systemic risks. Examples of permissible data include user engagement histories, content recommendation data, and content moderation archives. Significantly, Article 15(3) of the Delegated Act prohibits practices such as archiving or deletion requirements that could undermine the integrity of research.[14]

The vetting process for researchers is a key component of the framework. Article 40(8) of the DSA specifies eligibility criteria such as affiliation with recognized research organizations, independence from commercial interests, and adherence to data protection standards. National Digital Service Coordinators (DSCs) bear significant responsibility in interpreting these criteria, with the Delegated Act allowing consultation with independent advisory mechanisms for guidance. This collaborative approach balances rigorous data security with the need for transparency and accessibility.[15]

Finally, the framework confirms that eligibility is extended to non-EU researchers provided they meet the requirements for studying systemic risks in the European Union. However, this must align with the GDPR's provisions for international data transfers, necessitating consultation with data protection authorities where adequacy decisions are absent.[16] This provision facilitates cross-border research and collaboration while ensuring that personal data protections remain intact, reinforcing the balance between global study and privacy compliance.

Mediators are also introduced to resolve disputes between platforms and regulators, where the platform disagrees with a decision by the DSC (paid for by the platform).[17] This framework stands in stark contrast to the legal landscape in the United States where researchers face lawsuits and other forms of intimidation and concerns as a new presidential administration begins in office.[18]

CHALLENGES

Significant challenges remain in fully realizing the potential of these measures. Platform resistance to sharing sensitive data – whether due to privacy concerns, business interests, or fears of reputational harm – has historically slowed implementation efforts. The vetting process for researchers, while necessary for security and compliance, may become overly bureaucratic, limiting timely access to data that is critical for studying fast-moving disinfo-ops. Additionally, definitional ambiguities surrounding “systemic risks” leave room for inconsistent enforcement across jurisdictions, creating uncertainty about the scope and depth of data access researchers can expect.

Further, while the Delegated Act for Data Access introduces key technical mechanisms, including data inventories and the DSA Data Access Portal, questions remain about how effectively these provisions will be enforced. Platforms may narrowly interpret their obligations, providing access only to limited or highly redacted datasets, which could undermine the ability of researchers to conduct meaningful analysis. Moreover, cross-border collaboration remains a challenge, as non-EU researchers must navigate complex GDPR restrictions and additional compliance measures when seeking access to European platform data.

CONCLUSION

The European Union's structured approach to researcher access under the Digital Services Act represents a landmark advancement in the fight against disinformation. By establishing legally binding obligations for platforms to share data with vetted researchers, the EU has set a global precedent for transparency, accountability, and independent oversight. Article 40 of the DSA, alongside GDPR safeguards and the voluntary Code of Practice on Disinformation, creates a framework that balances data access with privacy protection, ensuring that research efforts align with fundamental rights. These mechanisms not only enhance the ability to identify systemic risks but also enable the development of evidence-based policies to mitigate digital threats.

Despite the hurdles, the EU's commitment to researcher access represents a crucial step toward greater transparency in the digital information space. Unlike jurisdictions where platforms operate with minimal regulatory oversight, the EU has codified the right to study multiple online issues, establishing a model that could inspire similar initiatives in other regions. If successfully implemented and enforced, this framework has the potential to significantly improve understanding of information ecosystems, strengthen democratic resilience, and pave the way for more robust global governance of online platforms. Ensuring that these efforts translate into meaningful and sustained access will be critical in the coming years, as researchers, policymakers, and civil society organizations work together to combat the growing threats posed by digital disinfo-ops.

END NOTES

1 For a proposal to curb automated and synthetic activity, preserve privacy and promote human interaction, see S Hallensleben, Trust in the European Digital Space in the Age of Automated Bots and Fakes (European Observatory of ICT Standardisation, January 2022) <https://www.standict.eu/news/trusted-information-digital-space> accessed Dec 2024.

2 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data (GDPR) [2016] OJ L119/1.

3 European Commission, Strengthened Code of Practice on Disinformation (June 2022) <https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation> accessed Dec 2024.

4 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 (DSA) [2022] OJ L277/1.

5 P Voigt and A von dem Bussche, The EU General Data Protection Regulation (GDPR): A Practical Guide (Springer, 2017); C Kuner, L Bygrave, and C Docksey (eds), The EU General Data Protection Regulation (GDPR): A Commentary (OUP, 2020).

6 European Digital Media Observatory (EDMO), European Digital Media Observatory Working Group on Platform-to-Researcher Data Access Final Report (2022) 66-7, 105 <https://edmo.eu/wp-content/uploads/2022/06/EDMO-report.pdf> accessed Dec 2024.

7 ibid 37-57. The EDMO has proposed the establishment of independent intermediary bodies to mediate between researchers and platforms. These intermediaries would be responsible for certifying researchers, vetting their projects for compliance, and ensuring adherence to GDPR principles. This mechanism would create a layer of accountability, enabling data sharing without compromising privacy or security.

8 L Ginsborg, 'Automated Access to (Non-Personal) Data for Research Purposes on Disinformation under the Strengthened Code of Practice' (MediaLaws, 20 March 2023) https://www.medialaws.eu/automated-access-to-non-personal-data-for-research-purposes-on-disinformation-under-the-strengthened-code-of-practice/; DisinfoCode, The Strengthened Code of Practice on Disinformation (2022) (DisinfoCode, 2023) <https://disinfocode.eu/wp-content/uploads/2023/01/The-Strengthened-Code-of-Practice-on-Disinformation-2022.pdf> both accessed Jan 2025.

9 This public sharing of data has been integrated as obligation in the DSA (n 3) art 40(12). For analysis of how platforms have been complying with this legal obligation see C Hickey et al., Public Data Access Programs: A First Look - Assessing Researcher Data Access Programs Under The Digital Services Act (May 2024) 1–50 <https://assets.mofoprod.net/network/documents/Public_Data_Access_Programs__A_First_Look.pdf> accessed Dec 2024.

10 DSA (n 3) art 40(8).

11 ibid, art 26(1).

12 European Commission, *Draft Commission Delegated Regulation (EU) …/… supplementing Regulation (EU) 2022/2065 of the European Parliament and of the Council with regard to the rules and procedures on data access for researchers* (final version expected Q1 2025) <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13817-Delegated-Regulation-on-data-access-provided-for-in-the-Digital-Services-Act_en> accessed Dec 2024.

13 ibid, art 3. Caution: This regulation is in draft form and may be subject to change before its adoption and publication.

14 ibid.

15 See M Vermeulen, "Reading the European Commission's Proposed Implementation of DSA Article 40: Six Initial Observations on a New Framework for Research Data Access" Tech Policy Press (29 Oct 2024) <https://www.techpolicy.press/reading-the-european-commissions-proposed-implementation-of-dsa-article-40-six-initial-observations-on-a-new-framework-for-research-data-access/> accessed Dec 2024.

16 ibid. For instance, the EU has determined that an adequate level of data security exists for the countries of Argentina, Canada, Japan, New Zealand, South Korea, Switzerland, Uruguay, the UK, or the US.

17 Draft Delegated Regulation (n 12) art 13.

18 H Murphy, "Donald Trump's return sends shivers through the anti-misinformation world" Financial Times (24 Nov 2024) <https://www.ft.com/content/bfb404e8-aa7e-4795-a60c-454a310293cc> accessed Nov 2024.

THE GENEVA ACADEMY

The Geneva Academy provides post-graduate education, conducts academic legal research and policy studies, and organizes training courses and expert meetings. We concentrate on branches of international law that relate to situations of armed conflict, protracted violence, and protection of human rights.

DISCLAIMER

The Geneva Academy of International Humanitarian Law and Human Rights is an independent academic centre. Our publications seek to provide insights, analysis and recommendations, based on open and primary sources, to policymakers, researchers, media, the private sector and the interested public. The designations and presentation of materials used, including their respective citations, do not imply the expression of any opinion on the part of the Geneva Academy concerning the legal status of any country, territory, or area or of its authorities, or concerning the delimitation of its boundaries. The views expressed in this publication represent those of the authors and not necessarily those of the Geneva Academy, its donors, parent institutions, the board or those who have provided input or participated in peer review. The Geneva Academy welcomes the consideration of a wide range of perspectives in pursuing a well-informed debate on critical policies, issues and developments in international human rights and humanitarian law.

The Geneva Academy of International Humanitarian Law and Human Rights

Villa Moynier
Rue de Lausanne 120B
CP 1063 - 1211 Geneva 1 - Switzerland
Phone: +41 (22) 908 44 83
Email: info@geneva-academy.ch
www.geneva-academy.ch