



**HAL**  
open science

## Seeing in the dark: Towards a broad construction of the access to data provisions of the DSA

Beatriz Botero Arcila, Pedro Ramaciotti, Emma Cabale

### ► To cite this version:

Beatriz Botero Arcila, Pedro Ramaciotti, Emma Cabale. Seeing in the dark: Towards a broad construction of the access to data provisions of the DSA. *Internet Policy Review*, 2026, 15 (1), <10.14763/2026.1.2085>. <hal-05522872>

**HAL Id: hal-05522872**

**<https://hal.science/hal-05522872v1>**

Submitted on 23 Feb 2026

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons CC BY 4.0 - Attribution - International License



Volume 15 Issue 1



RESEARCH  
ARTICLE



OPEN  
ACCESS



PEER  
REVIEWED

## Seeing in the dark: Towards a broad construction of the access to data provisions of the DSA

**Beatriz Botero Arcila** *Sciences Po Law School*

**Pedro Ramaciotti** *CNRS*

**Emma Cabale** *ENS de Paris-Saclay*

**DOI:** <https://doi.org/10.14763/2026.1.2085>

**Published:** 19 February 2026

**Received:** 2 July 2024 **Accepted:** 16 December 2024

**Funding:** The authors declare that they received no funding for the writing of this project specifically. The authors, however, are researchers at the project DSA Decoded, funded by Project Liberty.

**Competing Interests:** The author has declared that no competing interests exist that have influenced the text.

**Licence:** This is an open-access article distributed under the terms of the Creative Commons Attribution 3.0 License (Germany) which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. <https://creativecommons.org/licenses/by/3.0/de/deed.en>  
Copyright remains with the author(s).

**Citation:** Botero Arcila, B., Ramaciotti, P., & Cabale, E. (2026). Seeing in the dark: Towards a broad construction of the access to data provisions of the DSA. *Internet Policy Review*, 15(1). <https://doi.org/10.14763/2026.1.2085>

**Keywords:** Social media, Digital Services Act (DSA), Transparency, Platform research, Data

**Abstract:** The Digital Services Act (DSA) is the most ambitious effort taken by liberal democratic nations to regulate social media platforms. One of the main ways it does this is by establishing various transparency obligations applicable to all platforms and search engines, as well as a specific transparency and data-sharing regime for the largest platforms and search engines, defined by the number of users. Specifically, Article 40 of the DSA grants vetted researchers access to data “for the sole purpose of conducting research that contributes to the detection, identification and understanding of systemic risks in the Union.” This article argues that Article 40’s requirement for the requested data to be “necessary and proportionate” to conduct a specific type of research may hinder effective research. Indeed, researchers have been denied broad access – or any access to data – on privacy or confidentiality grounds before (Bontcheva, 2024). Consequently, researchers have limited prior knowledge of social media impacts and thus may have limited knowledge about what data, exactly, they need. Drawing on cutting-edge social media research, we explain why vetted researchers may thus need broad access to social media data to meet the objectives of the DSA. More specifically, we argue that researchers need access to system-level data, meaning data that captures how an entire digital system or platform operates, not just the activity of individual users. Consequently, we propose an interpretation of the DSA’s data request requirements that would enable researchers to study the online political landscape of EU member states effectively.

## Introduction

The Digital Services Act (DSA, adopted on 19 October 2022 by the European Union) is the most ambitious effort taken by liberal democratic nations to regulate social media platforms and online search engines. The DSA is to a large extent a risk regulation that requires the largest platforms and search engines to identify the principal risks their operations pose to key interests of the European Union – such as democracy, children’s mental health, or fundamental rights (DSA, Recital 80) – and to adopt mitigation measures (DSA, Recital 79). It also establishes various transparency obligations applicable to all platforms and search engines, as well as a specific transparency and data-sharing obligations for the largest platforms and search engines defined in Article 33 of the DSA as those “very large platforms” (VLOPs) or “very large search engines” (VLOSEs) that have 45 million or more users in the EU. Additionally, Article 40 grants vetted researchers access to data of VLOPs and VLOSEs “for the sole purpose of conducting research that contributes to the detection, identification and understanding of systemic risks in the Union” (DSA, Article 40.4). The data sharing mechanism promises to enable the research community to better understand the effects of platforms on our societies. Most importantly, however, these measures seek to leverage the knowledge and capacity of researchers to ensure transparency and accountability over VLOPs and VLOSEs and the measures they take to mitigate those risks. It is thus central to the system and the success of the DSA (Loutrel, 2024).

Article 40, however, seems to be narrowly drafted. It establishes that researchers’ access to data will be “for the sole purpose of conducting research that contributes to the detection, identification and understanding of systemic risks in the Union”

(DSA, Article 40.4). Moreover, in order to access such data, researchers should demonstrate “that their access to the data and the time frames requested are necessary for, and proportionate to, the purposes of the research” (DSA, Article 40.8(e)). Previous commentators have noted that this leaves out important information (Iramina, Perel (Filmar) & Elkin-Koren, 2023). This is the case, for example, with social media data that can be used to detect early signs of natural disasters or pandemics (Chunara, Andrews, & Brownstein, 2012), or social media data that can be utilised for digital health research (Nebeker, Dunseath, & Linares-Orozco, 2020).

In this article, we argue that Article 40 should be broadly interpreted, to enable broad access to data and, importantly, access to system-level data. System-level data refers to platform information that describes the overall functioning, performance, and state of the platform during a given timeframe, by including aggregated, structural and other process-level data. System-level contrasts with the *user-level data samples* typically provided through APIs or keyword queries, which are narrow by design and presuppose prior knowledge of what to search for. Previous research has shown that tailored access to information, based, for instance, on a query defining the data request made by researchers (e.g., using keywords, specific phrases, or hashtags), is seldom enough to understand the systemic risks and other emergent behaviours and effects associated with social media platforms (Matias & Wright, 2022).<sup>1</sup>

We further show that researchers in Europe will require broad access to data and access to system-level data to improve the understanding of systemic risks on social media platforms. This is not only because our understanding of how social media platforms work is generally limited (Shapiro et al., 2021). In Europe, the additional challenge is understanding how social media dynamics interact with the particularities of the properties of European informational spaces, which are different from informational space of the United States, where most social media research comes from (Lorenz-Spreen et al., 2023). Consequently, as Article 40 of the DSA is implemented and utilised, EU researchers will have to request data with predominantly incomplete and partial knowledge of the vast and complex social media ecosystems hosted in platforms. In this article, we also argue that this knowledge gap hinders their ability to anticipate the specific data required for their research, or at least to do so narrowly, encapsulating the problem of un-

1. Note that, from a transparency and accountability perspective, measures that at first sight seem transparency enhancing, such as releasing code, or information concerning content moderation (such as the number of complaints they receive from users, or the posts platforms take down) – have important limitations (Narayanan, 2023).

known unknowns (Ellenberg, 2015).

Article 40 of the DSA foresees, however, that researcher's access to data be "necessary and proportionate" and be balanced against other interests, such as the protection of confidential information (DSA, Article 40.5 (b)). Thus, we explain why broad access to data, and to system-level data can be necessary and argue that a narrower interpretation of Article 40 could hamper the provision's own objective of enabling the understanding of how systemic risks occur on social media platforms, especially so in Europe.

To illustrate our argument, the article draws on previous research examining the consequences of social media in political competition (relevant to risks under Article 34.1(e)). While our examples address risks defined in the DSA that relate to politics and elections, similar arguments can be made about other risks, such as those related to public health and the protection of minors online. To do so, this article proceeds as follows. The next section presents the DSA's access to data provisions for researchers, as well as its objectives. The second section presents the challenges of auditing platforms in relation to systemic risks. The third section draws on the previous work of the European Polarisation Observatory (a project led by several top research institutions in the EU to analyse political phenomena on social media) to propose an operational interpretation of the "reasoned" data requests.

## **I. The DSA systemic risk approach to a healthier information environment and the central role of access to data**

This first section briefly presents the EU content moderation legal framework and the new obligations introduced by the DSA. Then it explains why access to data is a central part of its governance framework.

### **A. The DSA**

The DSA is an EU-wide regulation that entered into force in 2024. It is concerned with updating and creating new rules for online intermediaries and platforms to enable a safe and trusted online environment (DSA, Article 1). The DSA replaced the 2000 E-Commerce Directive (ECD) to address some of the newer risks and challenges brought about by relatively new online business models such as social media and online platforms (DSA, Recital 47). It maintained the baseline immunity from liability for illegal content hosted by internet intermediaries that charac-

terised the ECD, if intermediaries do not participate in its creation and remove it once they are made aware of it (DSA, Recital 22). In addition to this baseline regime, the DSA created new obligations, such as transparency reporting and establishing clear points of contact for their users for all platforms. Importantly, the DSA created special risk management obligations for the largest actors in the common market, the VLOPs VLOSEs, under the understanding that they may cause societal risks “different in scope and impact from those caused by smaller platforms” (DSA, Recital 76).

The DSA requires VLOPs and VLOSEs to assess the systemic risks they, and the use and misuse of their services, may cause regarding the dissemination of illegal content (DSA, Recitals 79, 80), the foreseeable impact of the service on the exercise of fundamental rights, (DSA, Recital 81) concerns related to the foreseeable negative effects of these services on democratic processes and public security (DSA, Recital 82), and concerns regarding foreseeable negative impacts on the protection of public or mental health (DSA, Recital 83). Providers of VLOPs and VLOSEs are subsequently also obliged to deploy the necessary means to mitigate the systemic risks identified in the risk assessments (DSA, Recital 86).

The DSA's risk assessment approach is thus a way to address the EU's version of the “gordian knot of platform content moderation” (Douek, 2020): The societal impact of social media content moderation, along with the risks associated with the spread of disinformation and other potentially harmful content, require action. Until now, content moderation decisions have been made primarily by the platforms themselves, yet these decisions have an important public impact. Platforms, however, lack democratic legitimacy to do so without accountability. At the same time, excessive government intervention is also detrimental to the guarantee of freedom of expression (Zeng & Brennen, 2023), and uniform, effective, and mandatory rules at the Union level are crucial to safeguard the functioning of the internal market (DSA, Recital 4). To address these difficulties, the DSA introduces a variety of procedural rules regarding how online platforms can make content moderation decisions. In particular, it requires them to conduct systemic risk assessments and adopt mitigation measures (DSA, Article 35). In addition, the DSA ensures that compliance with these rules can be monitored and assessed, including transparency, data-sharing and reporting obligations (see DSA, Articles 37, 39, 40). For example, VLOPs must now publish periodic reports on the content moderation they engage in, their use of automated tools, and information on the average monthly active recipients of the service in the European Union (DSA, Article 24). Importantly for our purposes, Article 40 provides that VLOPs and VLOSEs must grant access to

supervisory authorities and to vetted researchers upon a reasoned request (DSA, Article 40.4).

Lastly, the Commission and so-called “Digital Service Coordinators” (DSCs) are responsible for overseeing, enforcing, and monitoring compliance with the DSA (DSA, Article 51). DSCs have the competence to monitor and enforce compliance with the DSA by intermediaries established in their territory (DSA, Article 51). They are responsible for processing access to data requests, as explained in the next section (DSA, Article 40.4). The Commission enjoys exclusive competence to supervise, enforce, and monitor VLOPs and VLOSEs, and their enhanced obligations (DSA, Article 56.3).

## **B. The provision and procedure to grant researchers access to data**

Article 40 outlines the rules for granting researchers access to data. There are two main avenues to do so:

The first avenue requires researchers to submit substantiated applications to the DSC of establishment demonstrating their qualifications with the requirements established in Article 40.8 (DSA, Article 40.8). Researchers seeking access must, for example, be affiliated with a research organization recognised by EU law (DSA, Article 40.8 (a)), be independent from commercial interests (DSA, Article 40.8 (b)), and be capable of fulfilling data security and confidentiality requirements (DSA, Article 40.8 (c)). In their application, the researchers must also demonstrate “that their access to the data and the timeframes requested are necessary for, and proportionate to, the purposes of their research” (DSA, Article 40.8 (e)). The purpose must be solely for conducting research “that contributes to the detection, identification and understanding of systemic risks in the Union, as set out in Article 34, and to the assessment of the adequacy, efficiency and impacts of the risk mitigation measures pursuant to Article 35” (DSA, Article 40.8 (e)). The application should thus include, for example, a question tied to a particular systemic risk, as well as explanations of the data needed to investigate their question (Albert, 2022).

DSCs of establishment will grant researchers the status of “vetted researchers” for the specific research project of the application if they meet the requirements. In addition, they conduct a preliminary assessment on whether the “access to the data and the time frames requested are necessary for, and proportionate to, the purposes of their research” and that the results of that research project will contribute to the detection, identification and understanding of systemic risks in the Union

(DSA, Article 40.8 (e)). Subsequently, the DSCs of establishment will issue a reasoned request for data access to the provider of a VLOP or VLOSE, as requested by the researchers (DSA, Article 40.8 (e)).

Upon the reasoned request of the DSCs, Article 40.4 establishes that VLOPs or VLOSEs shall provide access to the requested data for the specified research within a reasonable period (DSA, Article 40.4). VLOPs and VLOSEs, however, can request the DSCs to ask for amendments (a) because they do not have such data or (b) because giving access to the requested data will lead to significant security vulnerabilities or affect the protection of confidential information, such as trade secrets (DSA, Article 40.5) In any case, requests for amendment must include proposals for alternative means to provide access to the requested data or other suitable data for the request (DSA, Article 40.6). The DSCs of establishment will decide on such requests within 15 days and communicate the decision (DSA, Article 40.6).

In July 2025, a delegated act was published laying down the procedures and technical conditions under which VLOPs and VLOSEs are to share data with vetted researchers (DSA, Article 40.13). The delegated act focuses on the steps to secure access and the technical conditions to ensure that data is shared safely and securely, such as the establishment of a data access portal (European Commission, 2025, Article 3). When considering the conditions for processing personal data, the delegated act establishes that “the processing shall take place only insofar as it is proportionate and necessary for the purpose of the data access process” (European Commission, 2025, Article 5). Additionally, the delegated act requires researchers to submit

*a description of the data requested, including format, scope, and where possible specific attributes (...) information on the necessity and proportionality of the access to data (...) information on the identified risks in terms of confidentiality, data security and personal data (...) a description of the research activities to be conducted with the requested data; (European Commission, 2025, Article 8 see also Article 10).*

The delegated act establishes that the Commission will host a common data access portal and requires researchers requesting data to submit a description of the data requested, as well as information on the “necessity and proportionality of the access to data” (Delegated Act, Article 3, Article 8). The final act no longer requires data providers to provide an overview of their data inventory, as presented in the Draft Act, a necessary and welcome measure to facilitate researchers’ access to da-

ta (Draft delegated regulation, Ares(2024)7652659, Recital 3, 12). The draft act also does not provide an interpretation of what 'necessary and proportional access to data' entails. As we will further discuss below, this reinforces the difficulty researchers will have in describing the data they need to conduct research and showing that the access is necessary and proportionate.

The second avenue to access data stems from an obligation that platforms must "give access without undue delay to data (...) provided that the data is publicly accessible in their online interface." (DSA, Article 40.12). Thus, VLOPs and VLOSEs should establish an Application Programming Interface (API), a connection for serving and fetching data between programmes or platforms to provide researchers with easy access to data that could otherwise be obtained through scraping, for example. This form of access is also available to researchers who meet the conditions to become vetted researchers, as well as those affiliated with not-for-profit bodies or other associations, as long as they are independent of commercial interests, disclose their sources of funding, and can fulfill the data security and confidentiality requirements (DSA, Article 40.12).

### **C. The importance and the limits of the access to data provisions**

The access to data provisions of the DSA have been considered a significant advance in social media transparency (Iramina, Perel (Filmar), & Elkin-Koren, 2023; Leerssen, 2021; Albert, 2022). Historically, and with few exceptions (Calma, 2023), dominant social media companies have been reluctant to facilitate access to data for researchers, which has also limited the possibility of conducting comprehensive research about social phenomena related to social media and understanding their broader societal impact (Leerssen, 2021). Indeed, control over data drives many social media companies' business models, and sharing it may risk their proprietary interests over that information. In some instances, social media companies and other stakeholders have also asserted that sharing data affects the data protection interests of their users. Importantly, however, by not sharing data, social media companies may have avoided enhanced scrutiny and public attention for failing to comply with existing regulations or the broader effects of their actions on the public interest (Iramina, Perel, (Filmar) & Elkin-Koren, 2023).

First, scholars and commentators have also highlighted some of the limits of Article 40 (Leerssen, 2021). First, the access to data provision is relatively narrow. Paddy Leerssen commented on an early draft of the DSA that it was problematic that researchers could only request data for researchers regarding "systemic risks," as defined by the DSA (Leerssen, 2021). Even if systemic risk is a broad and open-end-

ed category, it remains narrower than a neutral category such as “public interest,” which could cover research that extends to other topics of interest that may go beyond the enforcement of the DSA (Leerssen, 2021). Relatedly, Aline Iramina, Maayan Perel, and Niva Elkin-Koren have argued that by favouring a form of research that is oriented towards regulatory compliance, the DSA leaves out important areas of academic and scientific research, ranging from medicine, the humanities, and social sciences, that would significantly benefit from access to platform data (Iramina, Perel (Filmar) & Elkin-Koren, 2023; Elkin-Koren, Perel (Filmar) & Somech, 2024).

Indeed, the DSA explains that the data requested should be used “for the sole purpose of conducting research that contributes to the detection, identification and understanding of systemic risks in the Union, as set out pursuant to Article 34(1).” Recall that Article 34 creates the obligation for VLOPs and VLOSEs to identify, analyse, and assess systemic risks in the EU, which stem from the design or functioning of their systems and services (DSA, Article 34). In addition, the DSA establishes that the research at issue should be oriented towards “the assessment of the adequacy, efficiency and impacts of the risk mitigation measures pursuant to Article 35” (DSA, Article 40.2). This leaves out the possibility of researching smaller platforms that are not subject to the obligation to provide data under the procedure established by Article 40, but which may still be worthy research, as it is often in small platforms where extremist dynamics thrive (Zuckerman, 2024). It may also overlook the possibility of auditing and understanding how social media platforms create systemic risks and the effectiveness of their mitigation measures (DSA, Article 34, Article 40). This is so, unless these are construed as having direct consequences for compliance with the risk mitigation obligations, which, as our next section discusses, are broadly defined.

Second, the access to data requests will have to be balanced against the security, trade secrets, and confidentiality interests of platforms (Leerssen, 2021). Art. 40.2 provides that Regulators and DSCs should consider the rights and interests of VLOPs and VLOSEs and the recipient of their services, such as the protection of personal data, and the protection of confidential information such as trade secrecy (DSA, Article 40.2). The concern that these arguments can be abused seems to have been at least partially addressed by Recital 97, which explains that “consideration of the commercial interests of providers should not lead to a refusal to provide access to data necessary for the specific research objective pursuant to a request under this Regulation” (DSA, Recital 97). Regarding data protection, it is possible to assert a legal basis under the GDPR that allows researchers to process per-

sonal information for public interest reasons, or because they have a legitimate interest, or are complying with a legal obligation. However, researchers should still take measures to protect that data (Vermeulen, 2021). The delegated act establishes that access to data applications must include the measures and safeguards to mitigate risks in terms of confidentiality, security, and data protection (Delegated Act, Article 8(c)).

## **II. Systems complexity in the light of Article 40: Why understanding societal systemic risks requires broad access to data**

Article 40 of the DSA requires researchers to explain why the data that they are requesting is necessary and proportional for the proposed research. (DSA, Article. 40.8(e)). In this section, we show that there are two main challenges with this provision. First, we argue that researchers may find it complicated to identify *a priori* the data they require because limited knowledge about how social media platforms work, and the data they have, will prevent researchers from being able to name *a priori* what data they need. Second, we explain why research on systemic risks requires broad access to data, and access to system-level data. To do so, we proceed by explaining the two steps that researchers requesting access to data may have to go through: First, identifying a systemic risk, and then conducting research leading to its assessment. We show that the boundaries of what constitutes a systemic risk are indeterminate and unclear in the DSA and the literature. This may not always represent a direct obstacle for researchers' access to data, especially when they are interested in studying a risk that clearly fits the definition, but it may represent challenges for borderline cases. Second, and this is at the centre of our argument, even for systemic risks that are clearly defined, such as the spread of disinformation, researchers may face significant challenges identifying *a priori* the data they need to examine the associated risk.

### **A. What is a systemic risk?**

The DSA does not define systemic risks exhaustively. It is also not clearly defined in academic literature on social media regulation. The term is commonly associated with the regulation of financial systems or environmental regulation, and it is increasingly acquiring a dominant role in the regulation of digital markets and digital society (Efroni, 2021). In the financial sector, for example, systemic risks refer to the events that could trigger severe instability and lead to the collapse of a sector or industry (Scott, 2016). In the computational sciences, it has been defined as the risks of having interdependent or cascading failures in a network (Helbing,

2013). Within the literature on social media regulation, the question of when a risk becomes systemic is also not fully developed. Civil society and scholars have noted that the lack of precise definitions, both in regulatory documents and in academic literature, creates challenges for operators and enforcement, while also affording flexibility and giving room to experimentation (Sullivan & Pielemeier, 2023; Global Network Initiative, 2023).

As used in the DSA, systemic risks thus seem to be those impacts of social media on society that may have severe negative consequences from a societal perspective, including illegal content, fundamental rights, data privacy, freedom of expression, rights of the child, electoral processes, public security, and health. According to Recital 79,

“In determining the significance of potential negative effects and impacts, providers should consider the severity of the potential impact and the probability of all such systemic risks. For example, they could assess whether the potential negative impact can affect a large number of persons, its potential irreversibility, or how difficult it is to remedy and restore the situation prevailing prior to the potential impact.” (DSA, Recital 79)

Article 34 of the DSA, which establishes the obligation to “diligently identify, analyze and assess systemic risks stemming from the design or functioning of their service and its related systems,” offers some examples and guidance. An important systemic risk is the “dissemination of illegal content” (DSA, Article 34.1(a)), such as the dissemination of child sexual abuse material (DSA, Article 80), but so are negative or foreseeable effects on the exercise of fundamental rights (DSA, Article 34.1 (b)), negative effects on civic discourse, electoral processes, and public security (DSA, Article 34.1 (c)), and negative effects related to gender-based violence, public health, the protection of minors, and individual’s physical and mental well-being (DSA, Article 34.1 (d)). Recitals 80 to 83 provide further guidance on the potential implications of these risks. For example, Recital 80 explains that where dissemination patterns are such that “illegal content may spread rapidly and widely through accounts with a particularly wide reach or other means of amplification,” this dissemination of illegal content may constitute a systemic risk (DSA, Recital 80).

Indeed, some systemic risks will be easy to identify, for example, because the DSA mentions them explicitly or because the Commission will have issued guidelines about them. In March 2024, for example, the EU Commission published a first set

of Guidelines on recommended measures for VLOSEs and VLOPs to mitigate systemic risks online that may impact the integrity of elections (EU Commission, 2024). But platforms themselves may enjoy a “first player’s advantage” in defining what systemic risks are and how to evaluate them as they present their first risk assessments.

Several scholars and organisations have also highlighted that the lack of standard definitions, methodologies or benchmarks raises risks that the evaluation of systemic risks will not be rigorous, or easy to compare (Loi, 2023; Pielemeier, Jahangir, and Ross, 2024; Sullivan and Pielemeier, 2023; Botero Arcila, 2023). This same lack of clarity may undermine researchers’ access to data for the “detection, identification and understanding of systemic risks in the Union,” since some risks may be considered systemic by some, but not for everyone (DSA, Article. 40.4).

## **B. The challenge of understanding systemic risks once they are identified: Broad access and access to system-level data**

In this part, we build on the idea that research tends to focus on platform systems to explain why, even when a systemic risk is identified and recognised as such, evaluating its severity and dynamics is no easy task, which in turn complicates explaining “what data” researchers need.

The impacts and effects of social media on society are hard to understand because social media platforms are complex systems. This means that their impact arises in nonlinear ways from the aggregation of numerous actions such as user actions and algorithmic and other platform affordances, often in unpredictable ways. Take the example of virality: The patterns of information propagation and exposure (who sees what) on platforms emerge through the interaction of several factors: the design of the interface, user behaviour, content moderation policies, and, of course, the different algorithms curating and mediating content that eventually determine what is visible on social media (Narayanan, 2023). Researchers have shown that predicting virality is a difficult problem, among others, because user behaviour is a crucial and volatile factor (Narayanan, 2023). Who and when something gets shared results in cascades of information diffusion and exponential growth that are complex, and hard to predict (especially with partial data (Narayanan, 2023).

Nevertheless, the virality of content on social media can be studied by extracting actionable rules for platforms. This requires, however, broad access to system-level data. In a pioneer study on the spread of misinformation, Guess, Nagler, and Tucker (2019) showed that the spread of news content labeled as misinformation by fact-

checking agencies was primarily driven by highly polarised individuals (i.e., individuals whose positions on several relevant issues are distant from the mean of the whole population). To do so, Guess et al. linked survey responses from individuals with their data produced on social media, relying on a sample of 3,500 users (Guess, Nagler, and Tucker, 2019). This allowed them “to provide a comprehensive observational portrait of the individual-level characteristics relating to posting articles from fake news-spreading domains to friends on social media” (Guess, Nagler, and Tucker, 2019). Yet their approach also underscores the limits of such panel data: while it revealed individual-level correlates of misinformation sharing, it could not capture the broader network and algorithmic dynamics of virality – something that requires system-level data.

Later studies on the sharing of misinformation or disinformation have also relied on broad access to data to understand how misinformation spreads on social media. Some of these studies, for example, have found that individual polarisation is the strongest predictor of whether a user will share factually inaccurate or misleading information, even when compared to education and data literacy (Osmundsen et al., 2021; Guess, Nagler, and Tucker, 2019; Lawson and Kakkar, 2022). Osmundsen et al. combined psychological profiling of over 2,300 American Twitter users with an analysis of sharing behavior and sentiment across more than 500,000 news headlines. (Osmundsen et al., 2021). To access this data, the authors commissioned a 20-minute survey and asked for permission to scrape publicly available Twitter data on relevant content to understand the informational ecosystem of users in the survey panel (Osmundsen et al., 2021). This sizeable sample provided the authors with insights into patterns of information spread and user behaviour within that network.

When considering phenomena like polarisation – or to study how the spread of misinformation or disinformation is related to polarisation – the importance of broad access to data, or access to system-level data stems from the central insight that polarisation is a property of a system and not only of an individual. That is, polarisation of an individual is always a relational attribute, it refers to that individual's position when compared with other individuals in the system (e.g., comparing the position of stances of an individual with respect to the mean of a population; Barbera, 2015), either a societal system or a social network within a social media platform. In other words, when estimating the polarisation of online users in a sample, it is essential that the individuals, collectively, cover a broad spectrum of political stances, which is challenging to achieve without broad data access. Properties such as polarisation are called systemic properties. The measure of sys-

temic properties requires access to data that encompasses the whole or vast amounts of the system to see how individuals behave *vis-à-vis* each other. And to study social media, we argue here, researchers will require broad access to data to assess risks related to systemic properties. Accordingly, and as Leerssen highlights, when asked what sort of analysis vetted researchers could conduct, “many researcher commentaries tend[ed] to focus not so much on specific domains, harms or risks as much as they do on specific platform systems, such as content recommendation and amplification, content moderation, and targeted advertising. (...) recurring theme is the need to study how recommender systems work in relation to individual users or what Lewandowsky et al. refer to as ‘human-algorithm entanglement’ – how interactions between user and the platform recursively shape each-other and create feedback loops” several researchers mentioned platform systems, such as content moderation, content amplification, or “human-algorithm entanglement” (Leerssen, 2023).

Recent publications by Meta on the 2020 US Presidential election show that Facebook systematically computes political estimates on the whole US Facebook population (González-Bailón et al., 2023). Other studies investigating the diversity of phenomena related to political segregation and the influence of algorithms on these dynamics rely on estimating the political leanings of users, considering the totality of users on the platform as the scope of analysis (Bakshy et al., 2015). These estimations are typically made using numerical scales that represent ideological positions, ranging from “most conservative” to “most liberal.” Different users are defined as liberal in relation to each other based on, for example, previous content that they have shared. These estimates are then used to formulate questions and methods for measuring concepts like polarisation or segregation in political discourse. What this means for research access to data is that, to conduct systemic risk research, researchers will often need longitudinal and systemic data. These needs thus require a broad interpretation of the “necessary and proportionate” requirement of Article 40 of the DSA.

The research community in Europe has already underscored the necessity of broad access to data: In the April-May 2023 call for evidence in the context of the Delegated Regulation on data access provided for in the DSA, 32% of the respondents were researchers (Leerssen, 2023). One of the questions of the consultation was “What type of data, metadata, data governance documentation, and other information about data and how it is used can be useful (...) for vetted researchers for conducting research related to systemic risks and mitigation measures?” According to Leerssen’s summary of the feedback received by the Commission, the responses

mentioned several types of data: data related to users, accounts, and pages (such as individual-level content exposure and engagement histories, or associated profiling and labeling); data related to content; data related to content recommendation (such as technical documentation on algorithmic ranking systems); data related to ad targeting and profiling (such as data used to profile types and market segments); and data related to content moderation and governance (Leerssen, 2023).

Researchers also emphasised the need for historical and longitudinal access, as well as real-time access, and the importance of technical documentation that provides context about the data being disclosed (Leerssen, 2023). At the time of writing, this has been included in the draft delegated act (Draft delegated regulation, Ares(2024)7652659, Article 8). According to the summary of the feedback received, technical documentation for the data provided is important to make sense of the data and thus researchers should also have access to data that include information about how the data was collected, relevant variables in the dataset, and how the variables are defined and calculated (Leerssen, 2023).

### **III. The challenge of researching systemic risks of social media in Europe**

The last part showed that doing research and understanding the systemic risks of social media requires broad access to data and to system-level data. This part develops this argument by showing that developing comprehensive research on some of the systemic risks of social media in the EU requires broad access to data.

To illustrate why research on systemic risks in the EU poses distinct challenges, we focus on political polarisation and information segregation a phenomena directly included in the risks of Article 34, including risks to freedom of information. Because European political landscapes are more fragmented and complex than the US left–right spectrum, studying systemic risks across the EU requires analytical frameworks that capture this diversity and therefore depend on broad access to system-level data. We illustrate this through one example from research on online segregation and two examples from studies of political recommendations, which together underscore the centrality of system-level data for developing meaningful metrics and detecting systemic risks under the DSA.

#### **A. Online segregation and exacerbation of political polarisation**

Segregation is defined as the process by which access to content generated by one group is limited for members of another. It may take a multitude of forms, includ-

ing segregation along gender, age groups, geographical regions, socio-professional groups, or even political groups. At its most severe, online segregation poses systemic risks to freedom of expression and information, the right to equality, and media freedom and pluralism. These are all risks defined under Article 34 of DSA.

To make an effective risk assessment of online segregation, researchers need system-level data to analyse the continually emerging groups and the selective exposure they might face. For example, a well-known case of online information segregation involves the role of platforms' recommender systems, studied by researchers at New York University. There, Brown et al. (2022) explain that:

*(l)ess well-understood is the degree to which the hubs of online communities – online social networks such as Facebook, Twitter, YouTube, and Reddit – are to blame for the segregation of the public into ideological echo chambers. (...) Part of the challenge in reconciling this debate stems from data limitations. Existing academic research that finds no evidence of a recommendation algorithm effect typically relies on either user watch histories or some type of anonymized data scraping method, both of which make a careful analysis of platform-specific effects hard to measure. User watch histories cannot untangle platform-specific features like recommendation algorithms from user behavior, since all that is recorded is the final user decision which is endogenous to both individual behavior and platform features (Hosseinmardi et al., 2020; Chen et al., 2021). Datasets assembled via anonymous scraping methods – i.e., relying on APIs or using “headless” browsers to scrape platforms – disconnect the sophisticated recommendation algorithms from the information on which they rely to operate – prior user behavior – and are therefore of questionable construct validity (Ledwich, 2020; Ribeiro et al., 2020). (Brown et al. 2022)*

To help bridge the described gap, the authors conducted a novel survey of YouTube users who, in the Fall of 2020, navigated the platform following randomly assigned rules. This enabled the authors to document the recommendations they encountered (Brown et al., 2022). The significance of this survey lies in the fact that it is not possible to draw general conclusions solely from recommendation data (i.e., which content is recommended to whom and when). Instead, their survey provided access to additional data that allowed researchers to characterise the recommendations users encountered as the effects of the recommendation algorithm on the one hand, and the effects of user behaviour on the other (Brown et al., 2022).

In the context of risk assessments, this provides another example where researchers may need to analyse a large data set, beyond a narrowly defined phe-

nomenon, to provide a comprehensive evaluation. However, the particularities of the European political landscapes underscore the importance of access to system-level data, as in the previous example related to polarisation. Assessing how platform affordances and algorithms contribute to polarisation in the EU requires examining system-level data, identifying relevant forms of polarisation, and avoiding reliance on *a priori* definitions. Indeed, not all definitions for polarisation will be suited to EU countries, such as the predominant left-right angle used to study online polarisation in most studies (Lorenz-Spreen et al., 2023; Falkenberg et al., 2025). This predominant single-dimensional scale comes from the United States, where most studies come from. Indeed, the United States' political landscape is predominantly characterised (for the study of online social systems) by a binary Liberal-Conservative scale (Iyengar et al., 2019; Jost and Baldassarri, 2023). Examples of this adoption are numerous in studies of polarisation on Facebook (Bond & Messing, 2015; Bakshy et al., 2015; Gonzalez-Bailon, 2023), X/Twitter (Barbera, 2015), but also prevalent in research across most other platforms (Di Martino et al., 2024).

The situation is radically different in European countries. The academic consensus is that relative issue alignment, that is how stances on one issue predict those on other issues, is stronger in the US than in Europe (Iyengar et al., 2019; Bakker et al., 2012; Jost & Baldassarri, 2023). European political landscapes are many, and they have been shown to need several additional dimensions beyond the traditional Liberal-Conservative or Left-Right dimension that is typical of the US context (Bakker et al., 2012). Consequently, depending on the country, additional political dimensions are indispensable to capture phenomena such as polarisation and fragmentation. This includes measuring attitudes towards immigration, redistribution, liberal lifestyles, or towards the EU. In France, for example, dimensions capturing individual attitudes towards elites, institutions, and the EU are crucial in understanding observed online political behaviour and are irreducible to a Left-Right dimension (Ramaciotti Morales et al., 2021). The academic consensus is, on the contrary, that US political competition and stances among the public stances are significantly more aligned than in European politics (Iyengar et al., 2019; Bakker et al., 2012; Jost & Baldassarri, 2023). Therefore, studying the general nature of digital ecosystems across the EU requires developing frameworks to capture the political dimensionality of different national settings which, in turn, requires broad access to data and access to system-level data. Notably, this may not be as necessary where or when the scope and nature of systemic risk at issue (e.g., specific types of polarisation that are relevant to a given country) is well identified beforehand, as researchers will be better enabled to make more precise data requests.

While these more developed frameworks are developed, however, researchers conducting similar research on the risks associated with segregation and polarisation will need access to system-level data to identify relevant agglomerations and to organise the network's dimensions. This will be crucial to measure the diversity of dimensionalities that are relevant for their research projects. This may include information on all posts and users (rather than just data obtained through predefined text queries) that are part of a specific network and during a particular time period.

## **B. Political profiling in recommendations**

Article 26 of the DSA forbids platforms from presenting advertisements to users based on profiling using sensitive data, as defined by the GDPR, such as political opinion or affiliation. Profiling is the automated processing of personal data to predict aspects related to the data subject, such as their work performance, health outcomes, economic situation, or personality. It refers, specifically, to circumstances which can lead to legal or other meaningful effects for that person (Article 71, GDPR).

A narrow interpretation of political profiling refers to recommender systems trained on data for which an explicit variable of political preference is an attribute of platform users. However, recent research has shown that a wide variety of data, not directly containing political preferences, can be used during the training of machine learning models to allow the recommender model to develop political profiles of users within the trained model. For instance, Faverjon and Ramaciotti (2023) demonstrated that a wide range of recommender models employed by platforms learn and leverage users' political classifications (for example, into Left- or Right-leaning groups) solely by feeding information about preferred news media outlets during the training phase.

This raises two challenges for the implementation of Article 26 of the DSA and the prevention of systemic risks associated with the integrity of elections and democratic debate. First, platforms could intentionally circumvent limitations on using political data for targeting by indirectly training their recommender systems on signals that effectively achieve political targeting, without explicitly using labeled political data. They could then provide ad targeting services for political audiences by selling effective targeting percentages, without overtly feeding political information into the models. Second, even without intentional political targeting, platforms' recommender systems could lead to selective exposure and exacerbated ideological segregation simply by consistently showing content aligned with each

user's general political leaning, even if the platform is unaware that this is occurring.

Similarly, as in the example in Section III.A regarding informational segregation and political polarisation, assessing these scenarios and risks requires access to a broad range of data, including all posts and users within a specific online social network. This would allow researchers to build political scales for evaluating users and the recommendations they receive (Ramaciotti et al., 2022). In fact, recent quantitative research on online public opinion has shown that the data needed to establish these general political frameworks is difficult to define based on systemic risk alone. It is only through the analysis of system-level data – examining a large network of users on a platform – that relevant political dimensions or frames can be identified (e.g., positioning users or content on political axes for a national context in the EU), which then enables investigation of related systemic risks (e.g., whether certain content is isolated among specific segments of the population; Ramaciotti Morales et al., 2021).

## **Final recommendations and conclusion**

The DSA represents the most ambitious and comprehensive effort by liberal democracies to regulate social media platforms by operating on a risk-based approach. The DSA also establishes various transparency obligations for all platforms and search engines, along with a mandatory data-sharing regime for researchers. Article 40 provides for vetted researchers to access data exclusively for research aimed at detecting, identifying, and understanding systemic risks within the Union. These measures aim to ensure transparency and accountability for the platforms and the effectiveness of their risk mitigation strategies, thereby supporting the enforceability and success of the DSA.

In this Article, we aimed to demonstrate that a broad interpretation of Article 40 is required to allow researchers to get access to the data they need to do this work. That is, broad access to data that includes access to system-level data. This will enable researchers to gain a deeper understanding of the systemic properties of networks and comprehend how systemic risks emerge online. This comprehensive approach surpasses the limitations of many API rate limits, keyword searches, or curated lists typically shared by social media platforms.

We finalize by proposing a few recommendations for the implementation of Article 40, which may be especially useful for researchers submitting access to data requests and for DSCs evaluating the requests:

First, for researchers to submit a “reasoned” data request, they must be familiar with the data VLOPs and VLOSEs have. Platforms should thus be required to have available guidelines and libraries with a classification system for the data that they have. These guidelines should include information about non-private communication data (e.g., user interactions, content exposure, and engagement data), user account metadata (e.g., profile information, group memberships), and data governance documentation (e.g., platform governance decisions affecting user interactions). These data are relevant to the assessment of systemic risks, as demonstrated by Ramaciotti and Cointet's study on the impact of recommender systems on political polarisation, which required access to non-private communication data from French parliamentarians' Twitter accounts (Ramaciotti & Cointet, 2021).

Second, some types of research will require data at the system level. Researchers should explain this in their applications, but DCS's should interpret this as comprehended within the meaning of “necessary and proportionate” for systemic risk research, even if it ends up being a significant amount of data. Such data access could be provided with different security measures, for instance, in data vaults, allowing researchers to at least get an overview of the types of data mentioned above before deciding what they need. Future research might also quantify the amount of information – based on information theory – that cannot be obtained about properties of online social systems linked to systemic risks when limited by data access, especially restrictions on platform data.

Third, we recommend a “learning-by-doing” approach and a process that recognises researchers may need to revisit their data requests. Allowing researchers to modify their data access as their research progresses can be helpful. Similarly, creating a database of all data requests and related interfaces could inform future requests and empower smaller research teams and institutions by guiding them in making their requests.

---

## References

- Alba, D. (2022, June 23). Meta pulls support for tool used to keep misinformation in check. *Bloomberg*. <https://www.bloomberg.com/news/articles/2022-06-23/meta-pulls-support-for-tool-used-to-keep-misinformation-in-check>
- Albert, J. (2022, December 7). *A guide to the EU's new rules for researcher access to platform data*. AlgorithmWatch. <https://algorithmwatch.org/en/dsa-data-access-explained/>
- Ausloos, J., Leerssen, P., & ten Thije, P. (2020). *Operationalizing research access in platform governance: What to learn from other industries?* AlgorithmWatch. <https://algorithmwatch.org/de/wpc>

ontent/uploads/2020/06/GoverningPlatforms\_IViR\_study\_June2020-AlgorithmWatch-2020-06-24.pdf

Bakker, A. B., Tims, M., & Derks, D. (2012). Proactive personality and job performance: The role of job crafting and work engagement. *Human Relations*, 65(10), 1359–1378. <https://doi.org/10.1177/018726712453471>

Bakshy, E., Messing, S., & Adamic, L. A. (2015). Exposure to ideologically diverse news and opinion on Facebook. *Science*, 348(6239), 1130–1132. <https://doi.org/10.1126/science.aaa1160>

Barberá, P. (2015). Birds of the same feather tweet together: Bayesian ideal-point estimation using Twitter data. *Political Analysis*, 23, 76–91.

Bobrowsky, M. (2021). Facebook disables access for NYU research into political-ad targeting. *The Wall Street Journal*.

Bond, R., & Messing, S. (2015). Quantifying social media's political space: Estimating ideology from publicly revealed preferences on Facebook. *American Political Science Review*, 109(1), 62–78.

Bontcheva, K. (2024, April 18). Issues with data access and why they hinder transparency, accountability, and policy-oriented research. *European Digital Media Observatory*. <https://edmo.eu/blog/issues-with-dataaccess-and-why-they-hinder-transparency-accountability-and-policy-oriented-research/>

Botero Arcila, B. (2024, June). *Systemic risks in the DSA and its enforcement*. DSA Decoded. <https://www.dsadecoded.com/systemic-risks-in-the-dsa-and-its-enforcemen>

Brown, M. A., Bisbee, J., Lai, A., Bonneau, R., Nagler, J., & Tucker, J. A. (2022). *Echo chambers, rabbit holes, and algorithmic bias: How YouTube recommends content to real users*. SSRN. <https://doi.org/10.2139/ssrn.4114905>

Bundtzen, S., & Schwieter, C. (2023). *Access to social media data for public interest research: Lessons learnt & recommendations for strengthening initiatives in the EU and beyond*. Institute for Strategic Dialogue. <https://www.isdglobal.org/isd-publications/researcher-access-to-social-media-data-lessons-learnt-recommendations-for-strengthening-initiatives-in-the-eu-beyond/>

Calma, J. (2023, May 31). *Twitter just closed the book on academic research*. The Verge. <https://www.theverge.com/2023/5/31/23739084/twitter-elon-musk-api-policy-chilling-academic-research>

Chunara, R., Andrews, J. R., & Brownstein, J. S. (2012). Social and news media enable estimation of epidemiological patterns early in the 2010 Haitian cholera outbreak. *American Journal of Tropical Medicine and Hygiene*, 86(1), 39–45. <https://doi.org/10.4269/ajtmh.2012.11-0597>

Di Martino, E., Galeazzi, A., Starnini, M., Quattrociocchi, W., & Cinelli, M. (2024). *Characterizing the fragmentation of the social media ecosystem: From echo chambers to echo platforms*. arXiv. <https://doi.org/10.48550/arXiv.2411.16826>

Doek, E. (2020, May 11). *What kind of oversight board have you given us?* University of Chicago Law Review Online. <https://lawreview.uchicago.edu/online-archive/what-kind-oversight-boardhave-you-given-us>

Efroni, Z. (2021, November 16). *The Digital Services Act: Risk-based regulation of online platforms*. Internet Policy Review. <https://policyreview.info/articles/news/digital-services-act-risk-based-regulation-online-platforms/1606>

Elkin-Koren, N., Perel (Filmar), M., & Somech, O. (2024, March 19). *Unlocking platform data for*

research. <https://doi.org/10.2139/ssrn.4733788>

Ellenberg, J. (2014). *How not to be wrong: The power of mathematical thinking*. Penguin Press.

European Commission. (n.d.). *Digital Services Coordinators*. Retrieved <https://digital-strategy.ec.europa.eu/en/policies/dsa-dscs#:~:text=Digital%20Services%20Coordinators%20help%20the,enforcing%20and%20%20monitoring%20the%20%20DSA>

European Commission. (2024a). *The Digital Services Act: Ensuring a safe and accountable online environment*. [https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountableonline-environment\\_en](https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountableonline-environment_en)

European Commission. (2024b, March 26). *Commission publishes guidelines under the DSA for the mitigation of systemic risks online for elections*. <https://digitalstrategy.ec.europa.eu/en/news/commission-publishes-guidelines-under-dsa-mitigation-systemic-risksonline-elections>

European Commission. (2025). *C(2025) 4340—Delegated act on DSA data access*. <https://digital-strategy.ec.europa.eu/en/library/delegated-act-data-accessunder-digital-services-act-dsa>

European Polarisation Observatory. (2021). *European Polarisation Observatory (EPO)*. CIVICA Research. <https://www.civica.eu/research/research-toolsresources/civica-research-hub-horizon-2020/collaborative-research-projects>

Falkenberg, M., Cinelli, M., Galeazzi, A., Bail, C. A., Benito, R. M., & Bruns, A. (2025). *Towards global equity in political polarization research*. arXiv. <https://doi.org/10.48550/arXiv.2504.11090>

Global Network Initiative. (2023). *Discussion summary: Implementing risk assessments under the Digital Services Act*. <https://globalnetworkinitiative.org/wp-content/uploads/2023/06/Discussion-summary>

González-Bailón, S., Lazer, D., Barberá, P., Zhang, M., Allcott, H., Brown, T., Crespo-Tenorio, A., Freelon, D., Gentzkow, M., Guess, A. M., Iyengar, S., Kim, Y. M., Malhotra, N., Moehler, D., Nyhan, B., Pan, J., Rivera, C. V., Settle, J., Thorson, E., & Tucker, J. A. (2023). Asymmetric ideological segregation in exposure to political news on Facebook. *Science*, *381*(6656), 392-398. <https://doi.org/10.1126/science.ade7138>

Goodwin, A. M., Joseff, K., & Woolley, S. C. (2020). *Social media influencers and the 2020 US election: Paying 'regular people' for digital campaign communication*. Center for Media Engagement.

Guess, A., Nagler, J., & Tucker, J. (2019). Less than you think: Prevalence and predictors of fake news dissemination on Facebook. *Science Advances*, *5*(1), eaau4586. <https://doi.org/10.1126/sciadv.aau4586>

Hansen-Shapiro, E., Sugarman, M., Bermejo, F., & Zuckerman, E. (2021). *New approaches to platform data research*. NetGain Partnership. <https://drive.google.com/file/d/1bPsMbaBXAROUYYesaN3dCtfaZpXZgl0x/view>

Helbing, D. (2013). Globally networked risks and how to respond. *Nature*, *497*(7447), 51–59. <https://doi.org/10.1038/nature12047>

Iramina, A., Perel (Filmar), M., & Elkin-Koren, N. (2023). *Paving the way for the right to research platform data*. SSRN. <https://doi.org/10.2139/ssrn.4484052>

Iyengar, S., Lelkes, Y., Levendusky, M., Malhotra, N., & Westwood, S. J. (2019). The origins and consequences of affective polarization in the United States. *Annual Review of Political Science*, *22*(1), 129–146. <https://doi.org/10.1146/annurev-polisci-051117-073034>

Jingnan, H. (2023, February 9). *Twitter's new data access rules will make social media research harder*. National Public Radio. <https://www.npr.org/2023/02/09/1155543369/twitters-new-data-access-rule-s-will-make-social-mediaresearch-harder>

Jost, J. T., Baldassarri, D. S., & Druckman, J. N. (2022). Cognitive–motivational mechanisms of political polarization in social-communicative contexts. *Nature Reviews Psychology*, 1(10), 560–576. <https://doi.org/10.1038/s44159-022-00093-5>

Kayser-Bril, N. (2021, August 13). *AlgorithmWatch forced to shut down Instagram monitoring project after threats from Facebook*. AlgorithmWatch. <https://algorithmwatch.org/en/instagramresearch-shut-down-by-facebook/>

Lawson, M. A., & Kakkar, H. (2022). Of pandemics, politics, and personality: The role of conscientiousness and political ideology in the sharing of fake news. *Journal of Experimental Psychology: General*, 151(5), 1154–1177. <https://doi.org/10.1037/xge0001120>

Leerssen, P. (2023). *Call for evidence on the Delegated Regulation on data access provided for in the Digital Services Act– Summary & analysis*. European Commission. <https://digital-strategy.ec.europa.eu/en/library/digital-services-act-summary-report-call-evidencedelegated-regulation-data-access>

Loi, M. (2023). *Making sense of the digital service act: How to define platforms' systemic risks to democracy*. Algorithm Watch.

Lorenz-Spreen, P., Oswald, L., Lewandowsky, S., & Hertwig, R. (2023). A systematic review of worldwide causal and correlational evidence on digital media and democracy. *Nature Human Behaviour*, 7(1), 74–101. <https://doi.org/10.1038/s41562-022-01460-1>

Loutrel, B. (2024, March 21). *Intervention at Démocratie.ai: Lancement de l'Institut libre des transformations numériques de Sciences Po [Speech at Démocratie.ai: Launch of the Sciences Po free institute for digital transformation]* [Video recording]. <https://www.youtube.com/watch?v=Afwf4C5H4z0>

Matias, N., & Wright, L. (2022). *Impact assessment of human-algorithm feedback loops*. Just Tech. Social Science Research Council. <https://doi.org/10.35650/JT.302>

Metaxas, P. T., & Mustafaraj, E. (2012). Social media and the elections. *Science*, 338(6106), 472–473.

Narayanan, A. (2023a, March 9). *Understanding social media recommendation algorithms*. Knight First Amendment Institute. <https://knightcolumbia.org/content/understanding-social-mediarecommendation-algorithms>

Narayanan, A. (2023b, April 10). *Twitter showed us its algorithm. What does it tell us?* Knight First Amendment Institute. <https://knightcolumbia.org/blog/twitter-showed-us-its-algorithmwhat-does-it-tell-us>

Nebeker, C., Dunseath, S. E., & Linares-Orozco, R. (2020). A retrospective analysis of NIH-funded digital health research using social media platforms. *Digital Health*, 6, Article 2055207619901085. <https://doi.org/10.1177/2055207619901085>

Ó Fathaigh, R., Helberger, N., & Appelman, N. (2021). The perils of legally defining disinformation. *Internet Policy Review*, 10(4). <https://doi.org/10.14763/2021.4.1584>

Ojer, J., Cárcamo, D., Pastor-Satorras, R., & Starnini, M. (2025). Charting multidimensional ideological polarization across demographic groups in the USA. *Nature Human Behaviour*. <https://doi.org/10.1038/s41562-025-02251-0>

Pielemeier, J., Jahangir, R., & Ross, H. (2024, February 19). *Ensuring Digital Services Act audits deliver on their promise*. TechPolicy.Press. <https://www.techpolicy.press/ensuring-digital-services-actaudits-deliver-on-their-promise/>

Ramaciotti Morales, P., Cointet, J. P., Muñoz Zolotoochin, G., Fernández Peralta, A., Iñiguez, G., & Pournaki, A. (2022). Inferring attitudinal spaces in social networks. *Social Network Analysis and Mining*, 13(1), 14.

Ramaciotti Morales, P., & Cointet, J.-P. (2021). *Auditing the effect of social network recommendations on polarization in geometrical ideological spaces*. 627–632. <https://doi.org/10.1145/3460231.3478851>

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), Official Journal of the European Union 1 (2022). <https://eur-lex.europa.eu/eli/reg/2022/2065/oj>

Saltzman, M. (2017). Social media mining: Can we prevent the apocalypse? *Journal of Business and Behavioral Law*, 8(1), 19–29. <https://doi.org/10.5195/jbbl.2017.168>

Scott, H. S. (2016). *Connectedness and contagion: Protecting the financial system from panics*. The MIT Press.

Sullivan, D., & Pielemeier, J. (2023, July 19). *Unpacking 'systemic risk' under the EU's Digital Service Act*. Tech Policy Press. <https://www.techpolicy.press/unpacking-systemic-risk-under-the-eusdigital-service-act>

Vermeulen, M. (2021, July 27). *The keys to the kingdom: Overcoming GDPR concerns to unlock access to platform data for independent researchers*. Knight First Amendment Institute. <https://knightcolumbia.org/content/the-keys-to-the-kingdom/>

Zeng, J., & Brennen, S. B. (2023). Misinformation. *Internet Policy Review*, 12(4). <https://doi.org/10.14763/2023.4.1725>

Zuckerman, E. (2024, January 24). Social media is getting smaller—And more treacherous. *Wired*. <https://www.wired.com/story/social-media-is-getting-smaller-and-more-treacherous/>

Published by



in cooperation with

