

Political Communication Report Summer 2026 - Issue 33

“Political Communication Research under Data Constraints”

Open Sesame? Hopes and Limits of European Platform Data Access Regulation¹

Ulrike Klinger, University of Amsterdam

Jakob Ohme, Weizenbaum Institute for the Networked Society, Berlin

LK Seiling, Weizenbaum Institute for the Networked Society, Berlin

From Wild West to Regulated Access

For about two decades, regulators, scholars, and journalists treated social media platforms as emergent technologies — “*neuland*,” as German chancellor Angela Merkel infamously put it in 2013. The tech industry's narrative of ideologically neutral platforms, neither media nor subject to media regulation, requiring unregulated conditions to grow and deliver on their promises, dominated how democratic societies approached them. Even after harmful side effects of their business models became apparent around and after 2015 — a surge of mis/disinformation, polarisation, the decline of traditional journalism, a thriving ecosystem of radical and extremist actors as digital surrogates of far-right parties, to name a few — data access for researchers studying these heavily personalised, algorithmically curated “high-choice information environments” (van Aelst et al 2017) remained extremely limited (Bruns, 2021; Freelon, 2018). The global pandemic further contributed to opening regulators' eyes to the unhealthy discourse dynamics taking shape in these environments, and to the rise of “polarisation entrepreneurs” (Mau et al. 2026) exploiting an infrastructure that directed ad money and public attention towards the loudest, most controversial, and most infuriating voices. Around 2016, at least in Europe and other “middle powers” (Canada, Australia), regulators took first steps to rein in the most harmful platform effects — such as illegal content, copyright infringement — meeting open hostility and backlash from the tech companies in return. Drafting the newer generation of platform governance, including the Digital Services

¹ Copyright © 2026 Ulrike Klinger, Jakob Ohme, LK Seiling. Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at <http://politicalcommunication.org>.

Act (DSA, proposed in 2019, in effect since 2025), the Digital Markets Act, and the AI Act, required a considerable learning process.

For political communication researchers, the past two decades demanded methodological flexibility: innovating around data access restrictions, settling for incomplete and largely non-validatable datasets, and entering collaborative projects with tech companies in which the latter always held the upper hand. Data came from scraping, screenshots, commercial brokers, intermittent platform APIs, and — as those closed — data donations. This effectively hindered comparative research, as datasets varied in content, structure, and timeline. Cross-platform and longitudinal comparison was the hardest thing. Scholars also frequently operated in legal grey zones around scraping, data sharing, and open access. In short, access often depended on knowing someone inside a tech company (e.g. CrowdTangle), on having the resources to buy data from opaque brokers with mysterious names (e.g. Crimson Hexagon), on platforms voluntarily and temporarily opening APIs, or on team members who could scrape their way around restrictions. As a result, regulators often lacked the empirical evidence needed for effective governance, and moral panic — filter bubbles! — drove both public discourse and research alike.

With the legal right to platform data access established in the Digital Services Act, that era is over. A new period of regulated access has begun.

How It Works (in a Nutshell)

Data access is regulated in Article 40 of the DSA, distinguishing between public data (such as posts by parties or politicians) and non-public data (such as exposure-level data). What follows is a brief summary of the main provisions; for a comprehensive overview and practical guidance, see Seiling et al. (2025) and Ohme & Seiling (2026).

The right to data access applies only to very large online platforms and search engines with more than 45 million users in the EU. These include, unsurprisingly, X, Facebook, TikTok, and Instagram, but also platforms that have so far attracted little attention from political communication researchers: LinkedIn, Amazon, Booking, WhatsApp, and Wikipedia.² Public data — encompassing nearly everything researchers have tried to access over the past two decades — must be made available in real time under Article 40(12). While this has nominally applied since August 2024, in practice platforms are complying only reluctantly. Some platforms (re-)opened their APIs to researchers (Hickey, 2024). Among other consequences, this non-compliance led to the European Commission's €120 million fine against X in December 2025. Data disclosed by TikTok and YouTube as part of their commitments in the

² For a full list, see <https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses>

Code of Conduct on Disinformation³ show that acceptance rates of data access application vary between 34 % (TikTok) and 33 % (YouTube) for the second half of 2024 and 76 % (TikTok) and 61 % (YouTube) for the first half of 2025. While these disclosures do not include common reasons for rejections, non-representative results from self-disclosed access experiences⁴ indicated that platforms apply a very narrow understanding of the purpose limitation for DSA-based data access. According to this data, the average time between application submission and decisions taken by the platforms also varies substantially (69 days for X.com (n=17), 32 days for TikTok (n=13), and 13 days for YouTube (n=3))⁵.

Access to more sensitive, non-public data can also be requested under Article 40(4). This includes, but is not limited to, exposure-level data — what voters or vulnerable groups such as young people have actually seen while scrolling their feeds. Such data also enables scholars and regulators to scrutinise the self-reports platforms have been publishing under various regulatory frameworks. Many platforms regularly publish transparency reports detailing detected foreign interference or hate-related content; until now, those numbers could not be independently verified — one simply had to take them on faith. This also applies to data that, for instance, makes it possible to assess the adequacy, efficiency and impacts of risk mitigation measures, such as interventions or content moderation.

Access to both public and more sensitive data is subject to thresholds: Only vetted researchers may submit requests, and only for projects addressing "systemic risks in the Union," including "the dissemination of illegal content; actual or foreseeable negative effects on fundamental rights, civic discourse, electoral processes and public security; gender-based violence; the protection of public health and minors; as well as negative effects on people's physical and mental well-being" (Seiling et al. 2025: 9). While for public data the vetting is done by the platforms themselves, requests for non-public data have to be submitted through the European Commission's Data Access Portal⁶, the vetting is done by the local Digital Services Coordinators (DSCs), which likely implies an extensive process that can take several months. Researchers must store and manage data in protected, GDPR-compliant environments and publish results open access. Extensive documentation is required — including work contracts proving academic affiliation — and access expires after a fixed period.

What's Great About DSA Article 40

³ Accessible at disinfocode.eu/reports

⁴ Collected through the DSA40 Data Access Collaboratory's DSA40 Data Access Tracker, accessible at <https://www.soscisurvey.de/DSA40applications/>

⁵ Further results from the data access tracker can be accessed at <https://dsa40collaboratory.eu/tracker-insights/>

⁶ <https://data-access.dsa.ec.europa.eu>

Article 40 gives political communication researchers access to data they have never had before. Access to public data becomes easier, APIs may reopen, and data inventories will reveal what is actually available — likely inspiring research questions we have not yet thought to ask. All of this occurs within a clearly structured, transparent framework, backed by a legal right to access and an independent public authority. Here are the key improvements:

The DSC requests non-public data on behalf of researchers. Researchers submit access requests for non-public data through the European Commission's data access portal but never deal directly with platforms. That is the role of the Digital Services Coordinators (DSCs) — newly established, independent authorities in each EU member state tasked with implementing the DSA. Researchers can submit via their home country's DSC or via the DSC where the platform is located, which has the final say and, in most cases, is the Irish Coimisiún na Meán. This makes the Irish DSC a central player when it comes to researcher access to non-public data. The DSC checks submissions for eligibility and completeness, requests the data, negotiates amendments with platforms where needed. In practice, researchers no longer approach platforms alone and empty-handed — they have a legal right and a relatively well-resourced authority standing beside them. Whether this will impress the tech companies remains to be seen.

Platforms cannot simply say no. Once a DSC confirms that a data access request is legitimate, platforms cannot refuse outright. They may request amendments and must propose alternatives if the specific data is unavailable or cannot be accessed due to security or confidentiality concerns.

Data catalogues. A decade of restricted access has left researchers largely in the dark about what data platforms actually hold. Describing requested data precisely — especially given the proportionality requirement — involves considerable guesswork. As a remedy, the DSA requires platforms to publish data catalogues describing available data, its structure, and metadata. So far, however, only a few platforms are offering meaningful information.⁷ Even so, these catalogues alone represent a significant step forward and will undoubtedly open new research directions.

Orderly data access and management. The wild west era was not only suboptimal because of restricted access; researchers' data storage and management practices were often, to put it charitably, sloppy. The DSA data access regime changes this by requiring comprehensive documentation of data security and GDPR compliance. Even publicly available data — social media posts by politicians, for instance — contain personal data under EU law. A politician's Instagram or TikTok posts may feature identifiable individuals and may include information

⁷ See the catalogue provided by XNXX for a positive, albeit still incomplete, example (<https://info.xnxx.com/dsa-data-catalogue>); and the information provided by Meta for a negative example (<https://transparency.meta.com/researchtools/other-data-catalogue/>)

about political or religious beliefs, or even sexual preferences. Secure storage, access controls, and documentation are now mandatory.

Not limited to the EU. Although the DSA restricts access to non-public data to questions of "systemic risk to the Union," it does not restrict who may apply (for inspiration see Edelson 2026). The DSA will not help if you want to study election campaigns in the US, protest movements in Asia, or political polarisation in Africa. But researchers outside the EU may still request data for basic research on platform dynamics, cross-platform flows, affordance effects, or network structures. Communication flowing between the EU and third countries may also be eligible.

Remaining Challenges

Despite the advantages outlined above, the DSA is not a data fairy. Or to use a different metaphor: the open sesame works only for research on "systemic risks in the Union." That scope is fairly broad — particularly for political communication research and research on young people — covering vulnerable periods before elections, threats to democratic values, disinformation campaigns, propaganda, foreign interference, and hate and violence targeting politicians. But it is not a *carte blanche*.

A further challenge is funding. Researchers must provide detailed documentation of project funding, demonstrating independence and non-commercial intent — which means funding must already be secured before a data access request can be submitted. This risks a Catch-22: funding bodies typically expect data access to be confirmed before committing resources, to avoid project failure.

Finally, this new regime must survive contact with practice. It remains unclear how fully tech companies will comply with the DSA. Fierce legal battles may lie ahead, and despite the DSA's relatively strong sanctioning powers, the scale and accumulated wealth of these companies dwarfs the law's coercive reach.

The Biggest Challenge of All

This brings us to the key question: will researchers actually use this gateway?

Two things need to be understood. First, the era of voluntary data access is over. Platforms have closed their APIs and largely stopped collaborating with researchers. Scraping and data donations remain valuable, and are best used in a complementary way, e.g. to validate platform-shared datasets rather than as primary access routes. One reason is that they are essentially workarounds, and come with their own variety of challenges and pitfalls (e.g. van Driel et al. 2022). Second, DSA data access will only work if researchers start using it — building working

relationships with DSCs, learning to submit high-quality requests that meet eligibility criteria, and giving DSCs strong cases to win the legal battles on their behalf when platforms fail to comply. This is not the moment to wait and see, to let others go first, to shy away from a steep learning curve, or to give in to frustration with the process: “The risk at this juncture is not that regulatory frameworks are too ambitious, but that political and scholarly fatigue may lead to their premature abandonment” (De Vreese & Tromble 2026).

To place the DSA in a broader context, it represents a qualitatively new step in regulatory practice: for the first time, a major industry is under a legal obligation to share data with independent researchers. The nuclear, pharmaceutical, tobacco, and fossil fuel industries were never required to provide comparable access to data on potentially harmful societal effects. Let's not waste this historic opportunity.

For extensive information on DSA data access, FAQs, and guidance on submitting requests, visit <https://dsa40collaboratory.eu> or contact the authors.

References

- Bruns, A. (2021). After the ‘APIcalypse’: Social media platforms and their fight against critical scholarly research. In S. Walker, D. Mercea, & M. Bastos, *Disinformation and Data Lockdown on Social Platforms* (1st edn, pp. 14–36). Routledge.
<https://doi.org/10.4324/9781003206972-2>
- De Vreese, C., & Tromble, R. (2026). Moving Targets, Moving Politics: The State of Play in Social Media Data Access. *Political Communication* 43(04),
<https://doi.org/10.1080/10584609.2026.2681041>
- Edelson, L. (2026). What the DSA Means Outside Europe: Research Access and Its Limits. *Political Communication* 43(04), <https://doi.org/10.1080/10584609.2026.2665427>
- Freelon, D. (2018). Computational Research in the Post-API Age. *Political Communication*, 35(4), 665–668. <https://doi.org/10.1080/10584609.2018.1477506>
- Hickey, C., Dowling, K., Navia, I., & Pershan, C. (2024). *Public Data Access Programs: A First Look*. Mozilla Foundation.
https://assets.mofoprod.net/network/documents/Public_Data_Access_Programs_A_First_Look.pdf
- Mau, S., Lux, T., & Westheuser, L. (2026). *Trigger Points. Inequality and Political Polarization in Contemporary Society*. Bristol University Press.
- Ohme, J., Seiling, LK, (2026). Finally, Access: How Article 40 DSA Changes Platform Research in Practice. *Political Communication* 43(04),
<https://doi.org/10.1080/10584609.2026.2664157>
- Seiling, LK, Keller, C.I., Ohme, J., Klinger, U., & de Vreese, C. (2025). Data Access for Researchers under the Digital Services Act: From Policy to Practice. *Weizenbaum Policy Paper*. <https://doi.org/10.34669/WI.WPP/14>
- Van Aelst, P., Strömbäck, J., Aalberg, T., Esser, F., De Vreese, C., Matthes, J., ... & Stanyer, J. (2017). Political communication in a high-choice media environment: A challenge for democracy?. *Annals of the International Communication Association*, 41(1), 3-27.
- van Driel, I. I., Giachanou, A., Pouwels, J. L., Boeschoten, L., Beyens, I., & Valkenburg, P. M. (2022). Promises and Pitfalls of Social Media Data Donations. *Communication Methods and Measures*, 16(4), 266–282.
<https://doi.org/10.1080/19312458.2022.2109608>



[U. Klinger](#) is a Professor of Political Communication and Journalism at the University of Amsterdam, with over 15 years of experience studying online campaigns, information flows and discourse dynamics on social media platforms. Her research focuses on political communication, the transformation of digital publics, and the role of technologies in democratic societies. She is a Co-Principal Investigator in the #DSA40 Collaboratory, focusing on collaborative access to platform data under the EU's Digital Services Act.



[Jakob Ohme](#) (Ph.D., University of Southern Denmark) leads the "Digital News Dynamics" group at the Weizenbaum Institute, studying digital journalism's impact versus influencers and AI. His research focuses on news consumption, political engagement, and using digital trace data to advance political communication and journalism. He is a Co-Principal Investigator in the #DSA40 Collaboratory, focusing on collaborative access to platform data under the EU's Digital Services Act.



[LK Seiling](#) has an academic background in psychology, cognitive systems, and human factors. At Weizenbaum Institute since March 2020, they previously worked on GDPR-based privacy risk communication and on frameworks for the collection and processing of platform data in real and simulated environments. Since May 2024, they are responsible for the coordination of the DSA40 Data Access Collaboratory, which studies the implementation of the researcher data access provisions in the EU's Digital Services Act.