Institute for Strategic Dialogue

Sponsored by:
Federal Foreign Office

Access to Social Media Data for Public Interest Research:

Lessons Learnt and Recommendations for Strengthening Initiatives in the EU and Beyond

Sara Bundtzen & Christian Schwieter

About the Digital Policy Lab

The Digital Policy Lab (DPL) is an inter-governmental working group focused on charting the policy path forward to prevent and counter the spread of disinformation, hate speech, extremist and terrorist content online. It is comprised of representatives of relevant ministries and regulatory bodies from liberal democracies. The DPL aims to foster inter-governmental exchange, provide policymakers and regulators with access to sector-leading expertise and research, and build an international community of practice around key challenges in the digital policy space. We thank the German Federal Foreign Office for their support for this project.

About this Paper

As part of the DPL, the Institute for Strategic Dialogue (ISD) organised several working group meetings on the topic of data access between October and November 2022. The working group consisted of DPL members representing national ministries and regulators from Canada, France, Ireland, Slovakia, Switzerland, the US, and the UK. Participants also included representatives from civil society, academia, and industry. While participants contributed to this publication, the views expressed in this report do not necessarily reflect the views of all participants or any governments involved in this project.

Authors

Sara Bundtzen is an Analyst at ISD Germany, where she studies the spread of information manipulation by state and non-state political actors in multilingual online environments. As part of the Digital Policy Lab (DPL), Sara informs ISD's advisory work and analyses proposed pathways toward countering disinformation, influence campaigns, hate speech, and extremist content.

Christian Schwieter is a Fellow at ISD and a PhD candidate at the Department of Media Studies at Stockholm University, where he investigates the impact of European platform governance efforts on far-right activity on social media. Until 2023, he was Project Manager at ISD Germany, leading the multiannual German-language research project "Countering Radicalisation in Right-wing Extremist Online Subcultures", funded by the German Ministry of Justice. He also co-led the pilot phase of the Digital Policy Lab at ISD.

Editorial responsibility

Huberta von Voss, Executive Director ISD Germany

Acknowledgements

We would like to thank all participants of the working group, including experts from civil society, academia, and industry, for their contributions. We would like to give special thanks to the speakers as well as contributors to this paper for providing valuable insights, criticism and feedback: Ľuboš Kukliš (formerly Council for Broadcasting and Retransmission of Slovakia), Oliver Marsh (The Data Skills Consultancy), Chris Meserole (The Brookings Institution), Nina Morschhäuser (formerly Twitter Deutschland), Susan Ness (Annenberg Public Policy Center), Chris Riley (Annenberg Public Policy Center), Jack Pay (CASM Technology), Mathias Vermeulen (AWO Agency), Dr. Katrin Weller (GESIS). Meta staff also participated in the working group and provided feedback on this publication.

ISD | Institute for Strategic Dialogue

www.isdgermany.org

Table of Contents

Executive Summary

This Policy Paper reviews key lessons learnt from industry-academia partnerships and other types of pre-existing data access initiatives. The analysis further explores potential future avenues for international collaboration among liberal-democratic governments, with an emphasis on regulatory and co-regulatory framework emerging at the EU level. Throughout, the Paper provides recommendations applicable across multi-stakeholder approaches to support the alignment of government initiatives in theory and practice.

Key recommendations to ensure public scrutiny of social media platforms and safeguard public interest researcher access to platform data.

Enabling common data collection methods and data documentation practices:

- Public interest researchers and regulators should establish data management principles and practices to enable reproducibility, verifiability and peer review of research findings.
- Researchers and regulators should develop comparison values within and between platforms to allow for comparisons of content and user behaviour across platforms.
- Regulators should recognise the value of mixed methods approaches, including different data collection methods used by researchers, for understanding the wider implications of social media platforms for individuals and society at large.

Improving the value of transparency reporting:

- Companies, regulators and public interest researchers should enable more consistency and standardisation of transparency reporting by companies through the development of a set of common metrics and categories, whenever reasonable.
- When there are no clear categories of content, given distinct geographical, linguistic and legal contexts, companies should be transparent about the methodology used to categorise types of content.

Safeguarding company-sanctioned researcher access to machine-readable data:

- Companies and policymakers should ensure that data access regimes account for a nuanced approach to user privacy expectations. Publicly available data with no 'reasonable expectations' of privacy such as content that is publicly accessible on platforms' online interfaces should be made available via vetted API access and include metrics about reach, impressions and engagement.
- Companies should provide comprehensive public documentation about legitimate use-cases and research requirements to access API endpoints. It should be clearly stated what access public interest researchers can obtain from the API, and what types of use-cases are legitimate.
- Regulators and public interest researchers should scrutinise the reasons why companies impose certain limits on historical searches or caps on data volume. Regulators may ask companies for clarification on these limiting measures and, where appropriate, challenge them if they interfere with public interest research.

Safeguarding researchers use of crowdsourced data and data donations:

- Policymakers should establish legal protections for public interest researchers to investigate platforms, provided researchers implement appropriate data privacy safeguards.
- Companies should establish voluntary carve-outs in their Terms of Service to permit research using crowdsourced data collection or data donations via browser extensions, if researchers comply with data privacy safeguards, including obtaining informed consent from participants. Such compliance could be demonstrated to companies, for example by formal approval from relevant research ethics committees.

Aligning data privacy expectations across jurisdictions:

- Policymakers in both EU and non-EU countries should leverage existing data privacy safeguards stipulated by the General Data Protection Regulation (GDPR), in particular its special regime for data processing for research purposes.
- In this context, cross-border collaborations should build on the draft Code of Conduct on how platforms can share data for public interest research purposes, developed by the European Digital Media Observatory (EDMO) Working Group.

Enabling vetting procedures of public-interest researchers beyond the regulatory context:

- Policymakers and regulators should eliminate loopholes for unauthorised commercial, government or law enforcement access to data, while empowering independent public interest research.
- Though academic affiliation can serve as a gatekeeping function, vetting procedures should allow for non-academic public interest researchers to be eligible for data access.
- Policymakers and regulators should clarify the cross-border application of vetting procedures. International collaboration should focus on aligning and integrating mechanisms alongside those proposed by EDMO's draft Code of Conduct.
- Policymakers, regulators and companies should acknowledge that research projects can be time-sensitive and depend on timely access to data. Handling of such data access requests could be aligned with the approach of the crisis response mechanism of the EU's Digital Services Act.
- Policymakers and regulators should consider vetting procedures not merely for the sake of compliance with regulation, but for public interest research in general. Beyond the scope of disinformation and 'systemic risks', vetting should be open to public interest research that seeks to understand the impact of social media on society at large.

Establishing an independent intermediary body:

- Regulators should ensure that an intermediary body is itself complying with transparency standards to avoid conflicts of interest and ensure democratic oversight.
- Regulators should ensure that an intermediary body comprises sufficient research and technical expertise, including appropriate human resources, so it can evaluate the research aims, methodological and ethical standards, as well as technical and operational data privacy safeguards of data access requests.
- Policymakers, regulators and public interest researchers should encourage a transnational outlook of an intermediary body beyond the EU's regulatory context. In compliance with the GDPR, the body could facilitate indices of publicly available data for researchers outside the EU, including for example a centralised public store of data dictionaries and codebooks that specify and explain which types of social media data are available.

Introduction

Meaningful access to social media data for public interest research must constitute the foundation of any evidence-based digital policy initiatives that aim to create a safer and more open online environment. However, the relationship between tech companies, governments, researchers, and the public remains defined by an information asymmetry due to a lack of sufficient data access regimes and infrastructure.

Emerging data access regimes in the EU and beyond should help to overcome this asymmetry, first and foremost by allowing public interest researchers to gain a better macro-understanding of the types of content and user behaviour on social media platforms. A more comprehensive understanding of how social media platforms can shape public interaction and discourse is vital to enabling evidence-based policy debates as well as the implementation and enforcement of regulatory frameworks. It remains crucial to gather more evidence on the role and influence of platforms on broader societal issues that are threatened by the spread of mis- and disinformation, hate speech, conspiratorial and extremist content. Scholars such as Nate Persily have argued that access to social media data has become a prerequisite to investigating and understanding most contemporary problems "in the real world"[1] – whether in the context of election cycles, foreign interference, public health, or societal attitudes towards climate change, migration or LGBT+ rights.

Testimony and leaked documents provided by Meta whistle-blowers allege that the company has not always been effective in combating both individual- and societal-level risks of online harms, despite being made aware of these problems by its employees.[2] While most social media platforms publish transparency reports in some form, in part to comply with government regulation[3], they often do not offer a holistic and comparable understanding of advertising, content moderation and algorithmic recommender systems.

The research community continues to be faced with barriers that impede systematic investigations into platform systems and practices. Barriers may relate to technological features of the platforms, ethical and legal concerns regarding data privacy, or the fragmentation of content and user activity (and therefore data) across different parts of the platforms so that it cannot be analysed systematically. Philipp Lorenz-Spreen of the Max Planck Institute for Human Development observed, "We do not depend on the oil industry to be able to measure CO2, but we are dependent on Facebook to measure polarisation on Facebook."[4] Concerns over violations of user privacy, particularly in the aftermath of the *Cambridge Analytica* scandal, slowed down the process of building the necessary infrastructure to access social media data.

Meaningful data access to platforms across the online ecosystem would allow for independent oversight and open avenues for public scrutiny, but any data access framework must safeguard user privacy in its design. Ultimately, data access for public interest researchers should enhance democratic decision-making, and ensure regulatory interventions are fit for purpose, proportionate and do not set precedents that could threaten fundamental rights of privacy and freedom of expression.

The aim of this Policy Paper is threefold:

1. To review key lessons learnt from industry-academia partnerships and other types of existing voluntary initiatives.
2. To explore potential future avenues for international collaboration among liberal-democratic governments, especially in the transatlantic partnership, with an emphasis on regulatory and co-regulatory frameworks emerging at the EU level.
3. To provide targeted recommendations applicable across government initiatives to support the alignment of approaches in theory and practice.

Lessons learnt from industry-academia partnerships and practices

Scholars from a range of academic disciplines have proposed research questions that could be better investigated if social media platforms enabled meaningful access to both user-generated data and platform data about moderation and recommendation systems, processes and outcomes.[5] The reasoning behind requesting such access is that platform data could be used as a proxy to assess multiple societal phenomena, as well as human behaviour, attitudes or opinions. Social media data can offer timely and large datasets compared with traditional, retrospective social science methods, especially in crisis situations such as a global pandemic.

This section highlights the methodological and ethical issues of accessing social media data, evaluating both the relevance of such data for research purposes and the emergence of diverse data access methods in the field. It looks at existing data access and transparency frameworks, including transparency reporting by companies, as well as academia-platform partnerships and practices.

Social media data for public interest research

A substantive debate about which types of social media data are required for what types of research questions should ensure sufficient context for policymakers and regulators, especially for those concerned with data privacy. Civil society organisations and academia should explain clearly why data is needed, to what ends it will be used and how their research would serve the public interest. This could, in turn, inform the formulation, adoption and enforcement of platform regulation.

Focusing on public interest research, we define and categorise the following types of data to contextualise what social media data we refer to when talking about types of access:

- **User-generated data** includes information about user activity on a platform. In theory, this comprises all user-generated content, such as posts and comments, as well as information about user signals, including likes, shares and other types of engagement. This data can be both public (e.g. a post shared publicly, or a comment made underneath a public post), or private (e.g. a post shared in private, smaller closed groups or group chats). Currently, several very large online platforms allow structured data access via Application Programming Interfaces (APIs) to this type of public data. Although not strictly user-generated, this data may also include descriptive statistics on the reach of posts, such as view count or post impressions.
- **Platform curation data** includes information relating to how platform systems, including human and algorithmic resources, moderate and rank (e.g. amplify or demote) user-generated content on a platform. This would include information about the platform's community guidelines (content moderation policies) and how they enforce them, including by means of content removal, content demotion or account suspension. Currently, transparency reports published by companies include aggregated information about content moderation decisions, sometimes specifying the type of content, the detection method, the type of restriction applied, and whether removal or suspension was due to the Terms of Service, legal requirements or government takedown requests.[6] This type of data is usually available in a non-machine-readable format. On a granular level, platform curation data could include signals or tags associated with types of content or accounts used for content moderation systems.[7]
- **Platform decision-making data** includes information about the internal decision-making processes of companies, including decisions regarding the platform's choice architecture, experiments conducted by ranking teams, or the methodology used for the evaluation of company metrics. For example, data would include information about the use of algorithmic recommender systems, including changes intended to increase certain types of engagement or forms of content, as well as the introduction of new features. Such data may be quantitative, for example, the outcome of experiments with ranking systems. Information about methodology and decision-making would be accessible in the form of qualitative information. Researchers would therefore likely rely on access to platform employees or company leadership, either through on-site inspections and interviews or access to internal documents, decision-making processes, and communication. In part, the 'Twitter Files' uncovered this type of data, albeit with caveats regarding its selectivity and verifiability.[8]

Based on an emerging body of research and the above categorisation of social media data, the Table 1 provides a non-exhaustive overview of public interest research questions. It reflects the argument that data access for researchers should not be *solely* based on demands for regulatory compliance. Public interest research may also cover research questions that do not fall within the scope of the contemporary digital policy debate, but that nonetheless advance our knowledge about human behaviour and society more broadly and may help to inform policy decisions in other areas outside of the regulation of online services. Data access regimes should therefore reflect on how social media research is not only of public interest when it seeks to directly inform digital policy and the regulation of social media platforms. The table thereby differentiates between research questions linked directly to compliance with platform regulation and broader research questions.

	Directly linked to compliance with current platform regulation efforts	**Indirectly linked to compliance with current platform regulation efforts**
Primarily user-generated data required	What is the prevalence of content that could be classified as "incitement to hatred" under the German penal code on Facebook? (Cf. Germany's Network Enforcement Act) How many views did video clips of RT and Sputnik broadcasting activities receive on YouTube one month prior and one month after the Russian invasion of Ukraine? (Cf. EU restrictive measures against Russian state-owned outlets)	How do discussions around the COVID-19 pandemic differ across Facebook and Twitter? What online news outlets are shared most prominently among German-language influencers on Instagram?

Primarily platform curation data required	How effective are warning labels from independent fact-checkers or authoritative sources in reducing the spread of misinformation on Twitter?[9] (Cf. EU 2022 Strengthened Code of Practice on Disinformation, Commitment 21) What types of users are more likely to be exposed to hate speech?[10] (Cf. EU Code of Conduct on countering illegal hate speech online) Do moderation decisions about what content is allowed on a platform affect some user groups disproportionately? (Cf. UK Online Safety Bill, 12 User empowerment duties) Are Instagram's 'Explore' page algorithms systematically amplifying the visibility of cyber-abuse content? (Cf. Australia's Online Safety Act 2021, Basic Online Safety expectations) What is the proportion of so-called 'superusers' that show hyperactive and abusive behaviour on Facebook? How can we measure the effect of 'superusers' on algorithmic feeds? (Cf. EU Digital Services Act, Article 34 Risk assessment)	How does historical user behaviour impact YouTube 'Shorts' recommendation algorithms? What is the role and impact of feedback loops between user behaviour and algorithmic recommendations? How do users adapt their posting behaviour in response to a changed choice architecture of a platform, for example, how did user interactions change when Facebook introduced the 'angry' reaction? To what extent does revealing the source of factual interventions affect the likelihood of users sharing misinformation?[11] Does context added to posts such as Twitter's Community Notes mitigate the spread of false and misleading information? To what extent do people from different points of view find them helpful? Does opting for a reverse-chronological timeline over an algorithmic feed alter the 'stickiness' of social media platforms?
Primarily platform decision-making data required	Are high-profile users treated preferentially in content moderation processes? (Cf. EU Digital Services Act, Article 15 Transparency reporting obligations) Are TikTok's algorithms intentionally demoting Black Lives Matter activists, i.e., reducing how frequently their videos appear on the 'For You' feed? (Cf. EU Digital Services Act, Article 37 Independent audit) Are users able to silence others through the misuse of moderation tools or through systemic harassment designed to censor certain viewpoints? (Cf. UK Online Safety Bill, 95 Investigations, 96 Power to require interviews, 97 Powers of entry, inspection and audit)	Is it possible to generate a quantitative estimate of the proportion of reach and engagement resulting from algorithmic 'amplification'? How could platforms and researchers assess user behaviour in a 'counterfactual' scenario, e.g. comparing user groups engaging with algorithmic vs. reverse-chronological feeds?[12] How are Meta's Oversight Board decisions received by company leadership? What effect do these decisions have on content moderation practices of other companies? How do ranking and product teams at social media companies decide on and use experiments to test and evaluate changes to the algorithms?

Table 1: Non-exhaustive overview of potential research questions linked directly or indirectly to compliance with current platform regulation. Note that the categories are not mutually exclusive. In reality, there is significant overlap between the types of data required and the types of questions that are directly or indirectly related to platform regulation.

The research questions are examples of topic areas that require data access to gather and understand the evidence of how social media platforms affect human interactions, behaviour and society at large. While public interest researchers use a range of methods to access and investigate social media data, there are certain barriers to conducting systematic, longitudinal (e.g. tracking user behaviour over time) and largescale studies of social media platforms.

Barriers to data access

Platforms may deliberately use technologies that restrict access to data or have other technological features which inadvertently create barriers to access. For example, certain content formats, particularly audio or audio-visual content, are not (yet) as amenable to systematic search and storage as text. In other instances, platforms offer services that are end-to-end-encrypted, whereby systematic data collection is impossible without access being granted by the sender or receiver. The emergence of blockchain technology may impose additional barriers. Systematically collecting data from blockchain-based platforms remains relatively unexplored territory. As partially blockchain-based platforms like Odysee do not have public research APIs, it remains unclear what data might become available and whether any further barriers might emerge during the process of data collection.[13]

What is described as fragmentation barriers may arise when relevant content that is publicly available is among vast amounts of data that cannot be searched quickly and systematically via platform-wide search functions or API. For example, Discord's public groups can only be searched server by server and not in a systematic way.[14] Furthermore, platforms may also use different metrics with varying definitions. For example, how individual 'views' are counted and what they describe can differ between platforms. It is therefore difficult to compare behaviour and content across platforms and construct validity of observations.[15]

Legal barriers may arise from the use of third party technologies to collect user data (such as scrapers or browser extensions) that are prohibited by the platforms' Terms of Service. There may also be the issue of platforms' retention of data and research demands for deleted data, especially data that platforms removed due to a violation of the Terms of Service. For example, some types of research require examining deleted content that could provide evidence of war crimes in conflict zones. There may be legal barriers to accessing deleted content such as legal provisions requiring companies to not retain deleted data or prohibitions on distributing illegal content.

More so, ethical problems can arise from varying expectations of user privacy and uncertainties in terms of how to distinguish 'public' from 'private' spaces online. For example, if researchers join a WhatsApp group, they could easily export the entire chat history as a text file. However, this poses several ethical concerns: how did the researcher join the group? Did they gain explicit permission from all the members to use the group's content for research (potentially leading participants to self-censor)? Are the group members unaware of the researcher in their chat, and therefore might not be consenting research participants? Did the researcher potentially gain access to the group via deception?

In the context of these diverse barriers, researchers have been employing diverse research methods and approaches to collect and analyse social media data. For example, researchers may survey users, use sock puppet accounts to investigate features from the perspective of users with different characteristics, or use data donation tools that allow users to voluntarily give them data directly. Alternatively, researchers may attempt to scrape data from a platform (for example, services such as those provided by ScrapeHero have allowed researchers to pull in historical Twitter data using web-scraping), and risk violating platforms' Terms of Service.[16] Other research approaches include digital ethnography, a well-established school of research methods that involves deep and sustained involvement with a community. Researchers may take a more 'human' approach by joining, participating in and observing online spaces as forms of community. This approach does not seek to produce larger volumes of data required for quantitative approaches and is more suitable for studying niche subcultures that require immersion.[17]

Another consequence of access barriers is that social media research, especially in the context of mis- and disinformation studies,[18] often lacks common quality standards for data collection as well as documentation practices. The lack of documentation practices can lead to a lack of transparency and verifiability, resulting in difficulties of advancing cumulative research and peer-reviewing analytical results.[19] The Governance Laboratory (GovLab) emphasised, "One of the key challenges of our data age actually lies in a persistent failure to re-use data responsibly for public good."[20] Moreover, the development of best practices continues to be impacted by the changing nature of social media data, for example, regarding the emergence of smaller platforms or de-centralised networks such as the Fediverse in which servers are hosted by a multitude of individuals rather than a company. Decentralisation may result in further fragmentation, reducing opportunities for systematic data access.[21]

Recommendations:

- **Public interest researchers and regulators should establish common data management principles, practices and methodologies to enable reproducibility, verifiability and peer review.** Data documentation should enable critical reflection of all aspects of how data is collected, prepared, handled, stored and shared.[22]

- **Public interest researchers and regulators should develop comparison values within and between platforms to understand which content is successful and how success is measured and to be able to draw comparisons of behaviour and content across platforms.** Simply put, how would a total number of likes on a large platform compare relatively to the total number of likes on another smaller platform. Such effort could support the development of public indices of comparison values of platform data.[23]

- **Regulators should recognise the value of mixed methods approaches given the range of platforms.** Data access mechanisms should acknowledge that the use of diverse data collection and analysis methods, for example, ethnographic monitoring, crowdsourced data or user surveys, can be necessary to complement automated access. Mixed data collection methods can help to generate a more comprehensive picture of the societal impact of social media as public interest researchers consider the wider implications of user experiences, including information processing and media consumption practices.

Transparency reporting (disclosure by default)

Transparency reports published by companies are public reports that usually contain non-machine-readable information about, or limited quantitative descriptions of, platform curation data and the platform's content moderation practices. For example, as part of their commitments under the EU's Strengthened 2022 Code of Practice on Disinformation[24], Signatories to the Code, including companies like Meta, Twitter and Google, publish reports in PDF as well as CSV and JSON formats, albeit with limited usability.[25]

Transparency reporting emerged in the mid-2000s as an industry response to concerns from civil society about the relationship between tech companies and governments. In 2010, Google became the first major tech company to publish a transparency report, then called the 'Government Requests tool', covering governmental requests for both user data and content removal.[26] In 2018, human rights organisations, advocates, and academic experts developed and launched a set of principles for how best to obtain meaningful transparency and accountability around platforms' moderation of user-generated content. The "Santa Clara Principles on Transparency and Accountability in Content Moderation" presented recommendations for platforms to "ensure that the enforcement of their content guidelines is fair, unbiased, proportional, and respectful of users' rights" and have been signed by twelve tech companies, including Apple, Meta, Google, Reddit, Twitter and Github.[27]

In 2020, the *Open Technology Institute* at the think-tank *New America* published a comprehensive tracking tool, reflecting data published by six platforms via transparency reports, to assess the practice of transparency reporting around content moderation.[28] The *Open Technology Institute* notes that transparency reports have become industry-wide best practices and mechanisms for companies to respond to public pressure by showcasing how they are tackling content moderation issues, for example, in topic areas such as COVID-19 or election mis- and disinformation. Companies such as Meta, Google, Twitter, TikTok and Reddit have been publishing transparency reports that include data on a set of metrics. Frequently reported metrics include the number of removed items of content, suspended accounts, or appealed content. In addition, most platforms apply their own, service-specific set of metrics. Meta for example publishes information about prevalence, which is the percentage of all content views that were of violating content in a particular content category, as well as the so-called 'proactive rate', meaning the percentage of content that was identified and flagged by the company's tools before users flagged them. Metrics are reported on in line with a range of varying categories of content (e.g., 'Hate speech' or 'Terrorism/ Violent Extremism'). Furthermore, Meta publishes 'Adversarial Threat Reports' on the company's removal of adversarial networks for different policy violations including Coordinated Inauthentic Behaviour (CIB), Brigading, and Mass Reporting. In this context, additional transparency efforts include the CrowdTangle API access, shared with a smaller group of researchers who can apply both quantitative and qualitative analysis to disrupted operations without the need to manually go through large spreadsheets or search for archived posts.[29]

However, arbitrary and unclear categories of content can obscure potentially valuable insights. For example, YouTube reports its metrics on the category "spam and misleading content", obscuring the information on how "misleading content" is moderated and spreading on the platform. This practice risks limiting the value of transparency reporting. At the same time, standardisation of content categories is only possible to an extent given that many categories of speech lack a standardised definition that applies across national and legislative contexts; for example, there is no universal definition of "extremist content" or "sexual imagery" that could be applied across all contexts and services.

Still, if platforms have sole discretion to decide which content types they report on (and importantly which they do not report on) and how they calculate that data (what metrics they choose to apply), there is a risk that some platforms exploit their transparency reporting as a mechanism to purposely share only information that paints them in an overly positive light.

Recommendations:

- **Companies, regulators and public interest researchers should continue to work together to ensure more consistency and standardisation of transparency reporting through the development of a set of common metrics and categories, whenever reasonable.** When there are no clear categories of content, given the distinct geographical, linguistic, and legal contexts, platforms should be transparent about the methodology applied for categorising content. Such efforts should build on existing models for transparency reporting developed by academia and civil society.[30]

European Union: Digital Services Act (DSA)

The EU's new horizontal rules introduced under the DSA include several transparency reporting obligations. Specifically, Article 15 obliges intermediary services to provide for "meaningful and comprehensible information" about:

- the content moderation engaged in, including the use of automated tools;
- the measures taken to provide training and assistance to persons in charge of content moderation;
- the number and type of measures taken that affect the availability, visibility and accessibility of information, categorised by the type of illegal content or violation of the terms and conditions, by the detection method and by the type of restriction applied.

All online platforms will need to further report on:

- the number of orders received from authorities, categorised by the type of illegal content;
- the number of user complaints, the basis for those complaints, decisions taken, the median time needed for those decisions, and the number of reversed decisions;
- the use of automated means for content moderation, including a qualitative description, a specification of the precise purposes, indicators of the accuracy and the possible error rate, and any safeguards.

Article 42 specifies that very large online platforms (VLOPs) or very large online search engines (VLOSEs), covering platforms that have more than 45 million monthly active users in the EU, will need to report on the qualifications and linguistic expertise of the content moderation teams as well as the indicators of accuracy used, broken down by EU languages.

In addition to above transparency reporting obligations, Article 40 further obliges VLOPs and VLOSEs to grant data access to vetted researchers upon a "reasoned request" from a Digital Services Coordinator (i.e. national regulator). In the context of compliance with the regulation, vetted researchers would – through data access requests to the national regulators – gain data access in order to contribute to "the detection, identification and understanding of systemic risks".

Note: On 17 February 2023, companies including Google, Meta, Microsoft, TikTok, Twitter and Snapchat reported on their user numbers. While the DSA will be fully applicable for all services in its scope from 17 February 2024, VLOPs and VLOSEs will have to comply with the obligations under the DSA four months following their designation as such. Based on the user numbers provided, the European Commission officially designated the first set of 17 VLOPs and two VLOSEs on 25 April 2023.[31]

Company-sanctioned API access to machine-readable data

This section discusses access for public interest researchers to machine-readable data, usually provided via APIs. Such company-sanctioned access allows programmers and researchers from outside the company to retrieve data from company servers.[32] Most platform APIs currently require researchers to apply for approval before access is granted, although application processes range from submitting a short form to outlining a research proposal.

Given that different types of data raise greater or lesser data privacy concerns, this section reflects on the current debate about 'public' versus 'private' spaces online. It will first consider the case of the *Social Science One* project to highlight lessons learnt. A discussion on the vetting procedures of public interest researchers will be provided in the second part of this paper.

Case study: Social Science One

Social Science One, housed at the *Institute for Quantitative Social Science* at Harvard University, is one of the most well-known partnerships between social scientists and industry. In 2018, the project was launched to pilot a specific model of industry-academic partnerships, seeking to share Facebook data with academics to assess the "impact of social media on democracy" as a test case. The project established a "commission of distinguished academics" to act as a trusted third party, with "full access to the company's proprietary data and knowledge of what is needed by the academic community".[33] Research proposals must first have been reviewed by a university Institutional Review Board, or an international equivalent, and are subject to peer-review managed by the Social Science Research Council (SSRC). Proposals are also subject to review by the company's privacy and research review teams as well as external privacy experts that the commission identifies. The commission independently selects grantees who will receive "privacy-protected data" from Facebook.[34]

Initially, the research objective had been to disclose "almost all public URLs Facebook users globally have clicked on, when, and by what types of people, including links judged to be intentionally false news stories by third party fact-checkers".[35] However, *Social Science One* faced significant delays due to concerns over protecting user privacy. The *Cambridge Analytica* scandal, which began with a breach by an academic of a developer's agreement with Facebook (barring the sale of the data to for-profit companies), had revealed how much user data is collected by platforms and potentially accessible to third parties.[36] Following the scandal, Facebook was concerned about further exacerbating the public backlash regarding violations of user privacy on its platform, leading the company to only share a highly aggregated dataset with less utility than anticipated.

Ultimately, the dataset contained information about 38 million URLs that were shared more than 100 times publicly on Facebook (between January 2017 and July 2019). Facebook applied differential privacy although the dataset was already aggregated at the URL level, including aggregated data concerning the types of people who viewed, shared, liked, reacted to, and otherwise interacted with these links.[37] *Social Science One* explained that differential privacy "works by censoring certain values in the data and adding specially calibrated noise to statistical results or data cell values" to obscure "any individual's actions who may be in the data".[38] The project sought to solve the resulting statistical problems,[39] noting, however, that most conclusions drawn from the dataset were "more uncertain than if researchers had access to the original data".[40] Additionally, there were concerns about the reliability of the data itself. Facebook data scientists discovered that the URLs dataset neglected to include about a third of the US population. Specifically, the dataset did not include users for whom Facebook had not identified a political affinity, thereby likely leaving out many political moderates and others whose political views were not easily classified.[41] Nate Persily, co-founder of *Social Science Once*, emphasised that the project now serves as "a clarion call for the establishment of a legally sanctioned and regulated process that will simultaneously grant researcher access while ensuring government oversight to protect user privacy".[42]

Accessing 'public' data

As noted by the *Social Science One* project, how data access regimes define 'public' data impacts the potential user privacy risks of making that data more widely available for public interest research purposes. Data access regimes thereby need to consider the question of what content falls within high expectations of user privacy. Platforms may offer multiple features, functionalities and affordances, such as livestreaming, pages or public groups, that each imply different levels of 'publicness'.[43]

Current regulatory precedent suggests that for public interest research there is no 'reasonable expectation'[44] of privacy in social media data that is "publicly accessible in platforms' online interface".[45] Content circulating in fully public spaces, meaning those online interfaces of the platform that are available to all users (or potentially also non-users) of the platform, can thereby be considered to have no 'reasonable expectations' of privacy.

The EU's Digital Services Act stipulates that platforms are expected to give vetted researchers access to "public accessible data" that could include "aggregated interactions from public pages, public groups, or public figures, including impression and engagement data such as the number of reactions, shares, and comments without undue delay" – this level of access is informally known as the CrowdTangle provision. Mathias Vermeulen from *AWO Agency* asserts that it "would likely be impractical for companies and researchers to employ a procedure that is very different".[46]

In parallel, the EU's 2022 Strengthened Code of Practice on Disinformation, signed by among others, Google, Twitter, TikTok, Meta, Microsoft, Twitch and Vimeo, refers to "access, wherever safe and practicable, to continuous, real-time or near real-time, searchable stable access to non-personal data and anonymised, aggregated, or manifestly-made public data for research purposes". It notes that "manifestly-made public data" can include "accounts belonging to public figures such as elected officials, news outlets and government accounts".[47] Similarly, the New York University's (NYU) *Cybersecurity for Democracy* describes such data as "reasonably public" content including:

- "high engagement" content, such as:
  public posts that reach a certain level of virality; public posts in the largest public online forums, such as the Reddit feed r/wallstreetbets; public content from accounts with very large audiences, such as those of so-called influencers;
- public content from government bodies and officials, as well as official candidates for office, regardless of their prominence.[48]

The term "manifestly-made public data" used in the Code originates from the General Data Protection Regulation (GDPR), however, it is unclear how Signatories interpret this notion in relation to their own services.[49] Moreover, the Code notes that access to automated means should be "subject to an application process which is not overly cumbersome".[50]

Meta: CrowdTangle

CrowdTangle exclusively tracks "public content", comprising interactions/engagement (total number of reactions, comments and shares) on public Instagram accounts, Facebook Pages, public Facebook groups and sub-reddits on Reddit. CrowdTangle does not provide the text of comments, only the number of comments, not differentiating between whether the comment was in response to the post, or in response to a comment on the post. CrowdTangle also does not track:

- Reach (unique number of people who saw a post at least once);
- Impressions (number of times a post was seen);
- Revenue;
- 1-Minute Video Views (number of times a video was played for at least 1 minute, excluding time spent re-playing the video);
- Link Clicks (number of times people clicked on a link (or the post itself);
- Any demographic information (age, gender, etc.) on the post or page-level;
- Whether or not content has been fact-checked.[51]

Researchers have criticised the lack of metrics that are being tracked.[52] In 2021, the CrowdTangle team within Meta was disbanded, with dozens of employees either quitting or getting new assignments in other parts of the company.[53] In January 2022, CrowdTangle stopped accepting new user applicants, citing "staffing constraints" that have not been addressed since. Researchers who can still access the API reported that it has not been updated in 16 months.[54] Instead, Meta increasingly focused on selective disclosures, publishing the Widely Viewed Content report every quarter that shares data on views and viewers of content in the Feed in the United States,[55] that relies on the reach metric – and thereby cannot be scrutinised by external researchers.

Data access for public interest researchers should acknowledge that there are grey areas of content that lie between "publicly accessible data" and non-public data. The *Center for Democracy & Technology (CDT)*, for example, uses the term 'semi-public' to refer to data that is not public in the sense that it is made available to any user of a service, but that also is not sent directly to just a single user or very small number of users.[56] Examples of such content would include Discord channels, Facebook closed groups, invite-only Telegram channels, Slack channels, or large WhatsApp groups. For example, content posted in a closed group that contains millions of members is available to large parts of the public but is not entirely public.

Furthermore, data access regimes should be aware that publicly accessible data may *in theory* lead to illegitimate use cases that invade user privacy, if not restricted to public interest research. Law enforcement and government surveillance of users, including in situations where such surveillance is not appropriate or warranted, could risk APIs being accessed for illegitimate purposes.[57]

Finally, some of the non-public data generated by the platforms such as historical data about user behaviour of extremist actors may be required for public interest research. Data access requests to non-public data would need to be assessed separately in vetting mechanisms, as such access certainly raises the risks of invading user privacy, revealing trade secrets or security measures used by platforms.

Recommendations:

- **Companies and policymakers should ensure that data access regimes account for a nuanced approach to user privacy.** User-generated data that raises no 'reasonable expectations' of privacy, such as content posted on public pages, public groups or content by public figures, should be made available via vetted API access, including data about reach, impressions and engagement metrics. Certain types of platform curation data could be made available in a machine-readable format via an archive of content moderation decisions. Other types of platform curation data relating to how algorithms rank content (such as demotion practices) as well as platform decision-making data would likely be obtained via other means (such as interviews with employees).

- **Companies should provide comprehensive public documentation about legitimate use cases and research requirements to access API endpoints.** It should be clearly stated what access researchers can gain from the API, and what use-cases are legitimate.

- **Regulators and public interest researchers should scrutinise the reasons why companies impose certain limits on historical search (e.g. only the last seven days of public posts) or caps on data volume (e.g. only 0.3 percent of all tweets per month).** Such considerations require relevant expertise to evaluate whether there are legitimate concerns about costs or user privacy that support allowing such limitations. Regulators may ask companies for clarification on these limiting measures and, where appropriate, challenge them if they interfere with public interest research.

Crowdsourced data and data donations

In addition to API access and transparency reporting, public interest researchers often use independent measures to gain access to platform data (without the company necessarily sanctioning it). Data donations and crowdsourced data involve volunteers installing a plug-in to report their data to a specific research project investigating a specific platform. Importantly, users give consent to their data being used for that specific purpose. Recital 33 GDPR recognises, "Data subjects [e.g. users] should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose." Data donations may provide insights of real user behaviour, as opposed to the use of sock puppet accounts that attempt to simulate the experience of users with certain characteristics or interests.

In July 2021, Mozilla published the largest-ever crowdsourced investigation into YouTube's recommendation system.[58] The dataset is powered by 37,380 volunteers across 190 countries who installed the *RegretsReporter* browser extensions for Firefox and Chrome. Mozilla stated that this "people-powered approach" captured the real lived experience of people who use YouTube and allowed some insight into the algorithm despite YouTube's unwillingness to provide data to researchers. Mozilla intentionally steered away from strictly defining what they consider as a *YouTube*

Regret to allow people to define the full spectrum of negative experiences that they have on YouTube. Using GeoIP lookup to determine from which country volunteers are accessing YouTube, researchers were able to monitor geographic and linguistic disparities. Mozilla also recognised methodological limitations of this approach, including selection bias (volunteers are a particular group of YouTube users), reporting bias (there may be many factors that affect whether a volunteer reports a particular video), as well as the observational nature, meaning that researchers are not able to confidently infer why something is happening (for example, researchers do not know why YouTube chose to recommend any particular video to any particular volunteer).

In September 2022, Mozilla published another study that used crowdsourced data of 22,838 participants to evaluate YouTube's feedback tools, looking at what happened over time to people's recommended videos after they had used one of the tools (e.g. the *Dislike* button).[59] Again, the study was carried out by participants that installed the web extension and opted into the experiment and data collection. The extension collected a range of data that was sent to Mozilla servers using Firefox telemetry. Among other things, data collected included a record of all uses of the *Stop recommending* button with timestamp and video ID; a record of all recommendations made by YouTube including timestamp, video ID, and type of recommendation; as well as a record of all interactions with native YouTube user control features. Notably, this methodology required significant technological, financial and human resources, including raising awareness about the extension and informing volunteers about their commitment to obtain informed consent. It is thereby unlikely to be feasible for smaller research organisations to conduct this type of crowdsourcing.

Meanwhile, Facebook has hindered the use of crowdsourcing methods in the past. Notably, NYU's *Cybersecurity for Democracy* developed *Ad Observer*, a web browser extension that copies the ads a user sees on Facebook and YouTube to a public database. It collects the advertiser's name and disclosure string, the ad's text, image, and link; the information Facebook provides about how the ad was targeted; when the ad was shown; and the browser language. It does not collect anything personally identifying. The tool aims to bring greater transparency to political advertising critical during presidential elections. However, Meta shut down the accounts of NYU researchers Laura Edelson and Damon McCoy, cutting off their access to Ad Library data as well as the CrowdTangle API.[60] The company cited concerns about user privacy arising from its settlement with the Federal Trade Commission (FTC), following the *Cambridge Analytica* scandal. However, the FTC clarified that the settlement did not prevent Meta from allowing such researcher access. Mozilla also argued the user privacy claims do not hold water. It conducted both a code review of the extension and examined the consent flow to ensure users understand exactly what they are installing. Mozilla concluded that the application of Meta's privacy policy was unjustified given the fact that the extension did not collect any personal information or information about participants' friends.[61]

United States: Platform Accountability and Transparency Act (PATA)

The PATA, introduced by then U.S. Senators Chris Coons (D-DE), Rob Portman (R-OH), Amy Klobuchar (D-MN) and Bill Cassidy (R-LA) in the 117th Congress (2021-2022), proposed to increase transparency around social media companies. It would give researchers at universities and non-profit organisations in the U.S. access to study data from the largest social media companies and provide public transparency on the "most widely shared posts, advertising, content moderation practices and recommendation algorithms".

The Bill further proposed to provide a limited legal safe harbour for researchers who collect data from social media platforms "through a covered method of digital investigation" and who take "reasonable measures" to protect user privacy.[62] Covered methods would include "the collection of data donated by a user, including through a browser extension or plug-in, where the donation is in connection with the project and with the user's explicit consent". Covered information would include "publicly available information", "information about ads, including the advertiser's name and disclosure string, and information the platform provides to users about how an ad was targeted", as well as any other category of information that would "not unduly burden user privacy".

Measures to protect user privacy would include measures taken to "avoid the collection and retention of non-public information that would readily identify a user without that user's consent", and to "prevent the theft and accidental disclosure of any data collected".

Recommendations:

- **Policymakers should establish legal protections for public interest researchers to investigate platforms, provided researchers implement data privacy safeguards.** A legal safe harbour should immunise researchers from civil liability. More so, it could prohibit a platform from barring a researcher's account or using technological measures to block access to researchers who qualify for such a safe harbour.[63]
- **Companies should establish voluntary carve-outs in their platforms' Terms of Service to permit research via methods such as crowdsourcing data, if researchers comply with data privacy safeguards, such as obtaining informed consent from participants.** For example, Mozilla explicitly states that it will not threaten or bring any legal action against anyone who makes a good faith effort to comply with its bug bounty programme. While the programme specifically encourages security research into Mozilla's websites, the company provides an example of good practice by clarifying legal protections for those researchers, promising not to sue researchers under any law or under the applicable Terms of Service and Acceptable Use Policy for their research through the bug bounty programme.[64]

Creating a data access infrastructure: towards international policy alignment

Given the inherently global dimension of the internet and social media platforms, liberal-democratic governments would benefit greatly from aligning their proposed transparency obligations and data access regimes. Aligning and integrating approaches does not necessarily require adopting new legislation, which often comes with significant political hurdles.

Susan Ness and Chris Riley have proposed a multistakeholder co-regulatory approach called "modularity" to foster greater internet governance alignment among liberal democracies notwithstanding different legal systems, regulatory appetites and societal norms. Through multistakeholder participation, modules are created to operationalise common tasks across borders, such as vetting researchers and approving their research proposals for access to platform data. A multinational, multistakeholder group of experts would draft standards and protocols for platform data access and form an independent body to operate the vetting system. Governments would formally or informally recognise the module as satisfying the vetting function under their regulatory frameworks, while enforcement would remain the province of government. Sunset provisions would ensure that the module remains updated and fit for purpose.

By avoiding multiple systems to achieve the same function, cross-border modules can conserve limited regulatory resources and improve platform compliance by reducing uncertainty due to different processes and rules. Moreover, cross-border participation in operating common functions helps to align and strengthen democracies.

European Union: 2022 Strengthened Code of Practice on Disinformation

The emerging data access infrastructure at the EU level comprises the obligations under the Digital Services Act (DSA) as well as commitments by Signatories of the 2022 Strengthened Code of Practice on Disinformation (CoPD) and the draft Code of Conduct on how platforms can share data with independent researchers while protecting users' rights, proposed by the European Digital Media Observatory (EDMO).

Complementing the DSA, tech companies including Google, Twitter, Microsoft, Meta, and TikTok have committed to make data available to enable research on disinformation under the CoPD. The ultimate purpose of the data access regime is different from that of the DSA, as access can be granted for any research purpose on "disinformation"[65], and is not limited to evaluating and auditing platforms' risk assessment and mitigation measures.

As part of their Commitments, Signatories launched a 'Transparency Centre' website in February 2023. The website should contain the Code's Commitments and Measures in an easy-to-understand and searchable manner. The website also includes an archive of Signatories' reports in PDF, CSV and JSON formats. These reports comprise qualitative reporting elements as well as quantitative "service level indicators" tied to the specific measures adopted under the Code. Furthermore, Signatories committed to work with a Task Force towards developing a methodology and the requisites for "structural indicators" designed to assess the effectiveness of the Code in reducing the spread of online disinformation, while doing so in a comprehensive and longitudinal way. In 2023, Signatories set up a Working Group to develop these "structural indicators" consisting of experts, including members of the EDMO Executive and Advisory Boards as well as the European Regulators Group for Audiovisual Media Services (ERGA).[66]

Signatories notably committed to "developing, funding, and cooperating with an independent, third party body that can vet researchers and research proposals". Such a body could likely merge efforts of the "independent advisory mechanism in support of sharing of data with researchers" proposed in the DSA and the "independent intermediary body" proposed by the EDMO Working Group.

Data privacy expectations

Privacy-compliant data access should consider privacy expectations across jurisdictions and aim for the highest existing standards. With the adoption of the GDPR, the EU arguably introduced the most thorough privacy legislation in the world.[67] Since then, there has been extensive debate regarding its implications for the sharing of platform data for public interest research purposes.

In 2022, the European Digital Media Observatory (EDMO) Working Group published a draft Code of Conduct, as intended under Article 40 of the GDPR, to clarify how GDPR privacy obligations apply in the research context.[68] The Working Group's twelve members — drawn from academia, civil society, and industry — met regularly to consider the legal, ethical, technical and scientific possibilities for facilitating data access.[69] Working Group members included representatives from Meta, Twitter and Google. As part of EDMO's final report, Meta and Twitter also submitted Concurring Opinions Letters.[70]

Importantly, EDMO's Working Group reiterates that the GDPR recognises the importance of research for our societies provides a special regime for data processing for research purposes, outlining legal roles, responsibilities and liabilities for both platforms and researchers. Specifically, the GDPR facilitates processing of personal data for research purposes in a "compatibility presumption" encoded in Article 5(1)(b), which establishes that processing of personal data for "purposes in the public interest, scientific or historical research purposes" is not considered incompatible with the initial purpose of the processing.

While the GDPR does not specifically define "research", Recital 159 states that, "The processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research."[71] The European Data Protection Supervisor further explained that this presumption of compatibility directly depends on the requirement to ensure appropriate technical and organisational safeguards, such as pseudonymisation and access limitations. Any secondary, compatible processing thereby must respect all other rules in the GDPR — from data minimisation to retention limitation to ensuring appropriate security.[72] The proposed Code of Conduct asserts that security measures must be appropriate to the nature and purpose of the processing and risks posed to the rights and freedoms of individuals. For example, typical risks recognised by the GDPR pertain to confidentiality (unauthorised access or disclosure), integrity (unlawful or accidental alteration) and availability (accidental or unlawful destruction). For researchers, the Code explains that if the objective of a project means that personal data are required, researchers should consider measures such as anonymisation or whether the data can be pseudonymised and if so, what steps against re-identification can be implemented to protect data subjects.[73]

Recommendations:

- **Policymakers in EU and non-EU countries should leverage existing data privacy obligations stipulated by the GDPR, in particular the special regime for data processing for research purposes, as an international standard of data protection safeguards.** In this context, EDMO's proposed Code of Conduct could serve as a starting point for cross-border collaborations of privacy-compliant data access regimes, both within and outside of the EU.

Vetted researchers

Automated and structured data access through APIs to public (as well as potentially semi-public and non-public) data should not only consider the data processing between researchers and platforms, but also the potential risks of unauthorised access (or other processing). Vetted researchers would thereby be prohibited from using data and information for commercial purposes or disclosing such data to unauthorised third parties.

While the DSA does not contain the details on the procedures for vetting researchers and providing access (to be clarified by the Commission in delegated acts), the regulation lists several conditions that researchers will need to fulfil for approval by the Digital Services Coordinator of Establishment, which is the regulator of the country in which a company has its headquarters (in many cases, this will be the Irish regulator).[74] Accordingly, eligible researchers would be considered when "affiliated with an organisation that conducts scientific research with the primary goal of supporting their public interest mission".

Similarly, EDMO's proposed Code of Conduct asserts that, based on the GDPR, "qualifying research" must aim for "the development of society's collective knowledge" and must be conducted by an "entity which has as one of its principal aims the conduct of research on a not-for-profit basis". Mathias Vermeulen from *AWO Agency* asserts that it would "likely extend to consortia of researchers that include non-EU based researchers and journalists, as long as a European researcher is the main applicant".[75] Researchers would further need to disclose their funding sources and demonstrate they are independent of commercial interests. In a vetting process, researchers would need to:

- describe the appropriate technical and organisational measures that will preserve data security and confidentiality requirements;
- justify why the data are necessary for their research purpose, and how the research would contribute to understanding either the "systemic risks in the EU" or the "adequacy, efficiency, and impacts of the risk mitigation measures";
- commit to sharing their research results publicly and free of charge;
- suggest their ideal data access format, and by which date they would like to have the data.

The DSA does not specify whether the researcher will need to be vetted before a data request can be submitted, or whether both processes can take place simultaneously. Vetting mechanisms could be based on a project-by-project basis, so researchers are approved depending on the specific data access request. Such a process would put less emphasis on who is requesting the data, but whether a particular research project itself proves suitable.

Recommendations:

- **Policymakers and regulators should ensure that vetting mechanisms eliminate potential loopholes for unauthorised commercial, government or law enforcement access, while empowering independent public research.** Thereby, though academic affiliation can serve as a gatekeeping function, vetting should allow for non-academic researchers to be eligible. Regulatory terminology such as "affiliated" or "associated" with a research organisation should ensure legal certainty as well as a broad applicability of public interest research, including researchers based outside the EU that can demonstrate they comply with the data privacy safeguards.

- **Policymakers and regulators should clarify the cross-border application of established vetting mechanisms.** International collaboration among liberal-democratic governments could focus on aligning and integrating vetting procedures alongside those proposed by EDMO's Code of Conduct.

- **Policymakers, regulators and companies should acknowledge that research projects can be time-sensitive, for example in crisis situations affecting public security or public health, and thereby depend on timely access to data to investigate content.** Vetting mechanisms should ensure efficient and appropriate handling of data access requests, whenever possible. Fast-tracked vetting mechanisms could be aligned with the DSA's crisis response mechanism, which will empower the European Commission to demand additional ad-hoc risk assessments from VLOPs and VLOSEs in times of crisis situations. Enabling timely vetting and access for researchers could also strengthen independent scrutiny of the effectiveness and proportionality of any measures taken under the crisis response mechanisms.[76]

- **Policymakers and regulators should consider vetting mechanisms not merely for the sake of compliance with regulation, but for broader public interest research.** Given that there are other instances during which researchers may want to request platform data, beyond topic areas of disinformation or 'systemic risks', vetting should be open to public interest research that seeks to understand the impact of social media on society at large.

An independent intermediary body: the regulator-researcher-platform relationship

Article 41 of the GDPR foresees the set-up of a Code Monitoring Body to observe the compliance with a Code of Conduct that outlines platform data access for researchers. In this context, the EDMO Working Group identified another gap in the status quo: namely, the absence of an independent intermediary body that can help oversee and implement the processes envisioned by the Code. The Working Group strongly recommends the creation of such a body for (a) certifying that researchers are qualified and competent to perform the research, (b) verifying that the research itself is qualified, and (c) providing these certifications to the platforms and any other appropriate parties.[77]

Streamlining review and certification processes and housing them in an independent intermediary body could reduce the burden placed on smaller, under-resourced universities and research institutions. Given the varying levels of resources and capacities among national regulators in the EU (and beyond), Mathias Vermeulen from *AWO Agency* notes that an intermediary body could further ensure sufficient context, skills and knowledge to assess different types of data access requests, research designs and methodologies.[78] In a similar manner, Julian Jaursch from *Stiftung Neue Verantwortung (SNV)* emphasises that national agencies would need a new "crop of experts", referring to the authorities that will take on the role of the Digital Service Coordinator (DSC) within the DSA framework. Jaursch underlines the need to attract experienced practitioners and academics from a variety of disciplines, while ensuring strong links with academia and civil society.[79] Ultimately, the evaluation of the feasibility, usefulness and relevance of data access requests will require interdisciplinary knowledge as well as diverse methodological expertise and data science skills.[80]

An independent intermediary body at EU level could help create such a community of experts, common standards of review as well as certification processes of the platforms' datasets, codebooks and technical systems. Beyond the EU, an independent intermediary body could support non-EU public interest researchers and research organisations. For example, the body could help to further international alignment through the coordination of vetting processes of data access requests. Such coordination should involve non-EU regulatory authorities and government agencies, including stakeholders in Switzerland, Australia, Canada, New Zealand, the UK and the US. For aligning transatlantic cooperation, policymakers could leverage existing working groups of the EU-US Trade and Technology Council.

Recommendations:

- **Regulators should ensure that an intermediary body is itself complying with transparency standards to avoid conflicts of interest and ensure democratic oversight.** This could include transparency registries documenting meetings with industry representatives, cooling-off periods for job changes between the body and industry and strong whistle-blower protections. The body could make publicly available information about whether and why a data access request has been granted or denied. Such information could also provide information about the number of requests as well as general information about the project proposals and types of data requested.

- **Regulators should ensure that an intermediary body comprises sufficient research expertise and human resources, so vetting processes can reasonably evaluate the research aims, methodological and ethical standards as well as technical and operational data privacy safeguards.** Sufficient resources are needed to avoid or pre-empt concerns leading to the denial of requests from platforms. Given the level of expertise and resources needed, scalability could be achieved through the regular exchange of knowledge with national regulators mandated to conduct the same tasks, including regulators in non-EU countries.

- **Policymakers, regulators and public interest researchers should encourage a transnational outlook via the intermediary body.** In compliance with the GDPR, the body could facilitate resources and indices of publicly available data for researchers based outside the EU. Such efforts should benefit the transparency of the research community as they could help to prevent duplicating workstreams. For example, the body, together with platforms and researchers, could build a centralised public store of data dictionaries and codebooks that specify and explain which types of social media data are available.

Conclusion

The volume of user-generated and platform curation data held by social media companies holds massive scientific value for public interest research, which seeks to better understand broader political and societal developments, trends and phenomena.

While certain legal, ethical and technological barriers to data access continue to restrict public interest research, researchers developed a range of methods for investigating user behaviour and content across different platforms, including methods to estimate the effects of algorithmic recommender systems on the amplification of certain types of content. At the same time, this paper demonstrates that accessing and sharing social media data can create new risks of jeopardising user privacy, without sufficient technical and organisational safeguards in place. Privacy expectations of users and relevant provisions in the EU's GDPR are thereby crucial when enabling access for public interest research purposes. Moreover, a data access infrastructure that ensures sufficient vetting and evaluation of data access requests by researchers should not only consider the data privacy obligations but allow for more clarity and coherence in the field of social media studies. This would also allow for better comparability and scrutiny of research findings by peers.

A multi-stakeholder process, involving platforms, policymakers, regulators and researchers should build on existing initiatives, rather than duplicate or reinvent efforts. The draft Code of Conduct proposed by the EDMO Working Group and the envisioned independent intermediary body offer a model that could be expanded to international collaboration among liberal-democratic governments beyond the EU. Policymakers, regulators and researchers must come together to levy their respective expertise, build trust between stakeholders, and ensure data access regimes are grounded in a robust legal framework in support of substantive social science research – not only to enable evidence-based regulation, but to advance scientific research in the digital era more broadly. Platform employees, including ranking and product teams, should be consulted throughout the process to ensure the feasibility and clarity of proposed data access regimes, particularly with an eye to any barriers to technical implementation.

Ultimately, all the recommended steps should ensure buy-in by relevant stakeholders, which, aside from clear accountability mechanisms, also demands goodwill by all those involved. The goal should be to foster a trustful, transparent and cooperative relationship between policymakers, regulators, researchers and companies. Such an effort can build a community of practice united by the mission to enhance public interest knowledge production by means of social media data and inform liberal-democratic governance efforts in the digital era.

Endnotes

1 Persily, N. (2022). Platform Transparency: Understanding the Impact of Social Media. Testimony Before the United States Senate Committee on the Judiciary – Subcommittee on Privacy, Technology, and the Law. Available at: https://www.judiciary.senate.gov/imo/media/doc/Persily%20Testimony.pdf.

2 See, for example, Haugen, F. (2021). Statement. United States Senate Committee on Commerce, Science and Transportation – Sub-Committee on Consumer Protection, Product Safety, and Data Security. Available at: https://www.commerce.senate.gov/services/files/FC8A558E-824E-4914-BEDB-3A7B1190BD49

3 See, for example, German Network Enforcement Act (*Netzwerkdurchsetzungsgesetz, NetzDG*) § 2 on reporting obligations. Available at: https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html

4 Kupferschmidt, K. (2023). Twitter's plan to cut off free data access evokes 'fair amount of panic' among scientists. *Science*. Available at: https://www.science.org/content/article/twitters-plan-cut-free-data-access-evokes-fair-amount-panic-among-scientists

5 See, for example, An Open Letter to Mr. Mark Zuckerberg: A Global Call to Act Now on Child and Adolescent Mental Health Science. *Oxford Internet Institute (OII)*. Available at: https://www.oii.ox.ac.uk/an-open-letterto-mark-zuckerberg/, or Pasquetto, I. et al. (2020). Tackling misinformation: What researchers could do with social media data. *Harvard Kennedy School Misinformation Review*. Available at: https://misinforeview.hks.harvard.edu/article/tackling-misinformation-what-researchers-coulddo-with-social-media-data/

6 For example, Article 15 of the Digital Services Act (DSA) requires transparency reporting to be categorised by the type of illegal content or violation of the terms and conditions. See here: Official Journal of the EU (2022). Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC (Digital Services Act). Volume 65. 27 October. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&from=EN

7 Elizabeth Hansen Shapiro et al. define such category as platform moderation data (moderation policies, moderated content data, data on Coordinated Inauthentic Behaviour), which is separate from "platform distribution data" (ad targeting data, search results data, content recommendation algorithms, and user experience data). See here: Hansen Shapiro, E., Sugarman, M., Bermejo, F., and Zuckerman, E. (2021). New Approaches to Platform Data Research. *NetGain Partnership*. Available at: https://drive.google.com/file/d/1bPsMbaBXAROUYVesaN3dCtfaZpXZgI0x/view

8 Coldewey, D. (2022). Musk's 'Twitter Files' offer a glimpse of the raw, complicated and thankless task of moderation. *Techcrunch*. Available at: https://techcrunch.com/2022/12/09/musks-twitter-files-offer-a-glimpse-of-the-raw-complicated-and-thankless-task-of-moderation/?guccounter=1

9 DiResta, R., Edelson, L., Nyhan, B., and Zuckerman, E. (2022). It's Time to Open the Black Box of Social Media. *Scientific American*. Available at: https://www.scientificamerican.com/article/its-time-to-open-the-black-box-of-social-media/

10 Ibid.

11 Pasquetto, I. et al. (2020). Tackling misinformation: what researchers could do with social media data. *Harvard Kennedy School Misinformation Review*. Available at: https://misinforeview.hks.harvard.edu/article/tackling-misinformation-what-researchers-could-do-with-social-media-data/

12 Thorburn, L. (2022). What Will "Amplification" Mean in Court?. *Tech Policy Press*. Available at: https://techpolicy.press/what-will-amplification-mean-in-court/

13 Matlach, P., Hammer, D. and Schwieter, C. (2022) Auf Odysee: Die Rolle von Blockchain-Technologie für die Monetarisierung im rechtsextremen Onlinemilieu. *Institute for Strategic Dialogue (ISD)*. Available at: https://www.isdglobal.org/isd-publications/auf-odysee-die-rolle-von-blockchain-technologie-fur-die-monetarisierung-in-rechtsextremen-onlinemilieu/

14 Guhl, J., Marsh, O. and Tuck, H. (2022). Researching the Evolving Online Ecosystem: Barriers, Methods and Future Challenges. *Institute for Strategic Dialogue (ISD)*. Available at: https://www.isdglobal.org/isd-publications/researching-the-evolving-online-ecosystem-barriers-methods-and-future-challenges/

15 Hammer, D., Rübbert, Z. and Schwieter, C. (2022). In the blind spot – How right-wing extremists use alternative platforms for radicalisation. Conference report on the 2021 Annual Conference for the project »Countering Radicalisation in Right-Wing Extremist Online Subcultures«. *Institute for Strategic Dialogue (ISD)*. Available at: https://www.isdglobal.org/isd-publications/in-the-blind-spot-how-right-wing-extremists-use-alternative-platforms-for-radicalisation/

16 Ahmed, W. (2019). Using Twitter as a data source: an overview of social media research tools. *LSE Impact Blog*. Available at: https://blogs.lse.ac.uk/impactofsocialsciences/2019/06/18/using-twitter-as-a-data-source-an-overview-of-social-media-research-tools-2019/

17 Guhl, J., Marsh, O. and Tuck, H. (2022). Researching the Evolving Online Ecosystem: Barriers, Methods and Future Challenges. *Institute for Strategic Dialogue (ISD)*. Available at: https://www.isdglobal.org/isd-publications/researching-the-evolving-online-ecosystem-barriers-methods-and-future-challenges/

18 Camargo, C. Q. and Simon, F. M. (2022). Mis- and disinformation studies are too big to fail: six suggestions for the field's future. *Harvard Kennedy School Misinformation Review*. September 2022, Volume 3, Issue 5. Available at: https://misinforeview.hks.harvard.edu/article/mis-and-disinformation-studies-are-too-bigto-fail-six-suggestions-for-the-fields-future/

19 Kinder-Kurlanda, K. E. and Weller, K. (2020). Perspective: Acknowledging Data Work in the Social Media Research Lifecycle. *Frontiers in Big Data*. Volume 3 – 2020. Available at: https://doi.org/10.3389/fdata.2020.509954

20 Verhulst, S. G. et al. (2019). Leveraging private data for public good. A Descriptive Analysis and Typology of Existing Practices. *GovLab*. Available at: https://thegovlab.org/static/files/publications/data-collab-report_Oct2019.pdf

21 Hammer, H., Gerster, L. and Schwieter, C. (2023). Inside the Digital Labyrinth: Right-Wing Extremist Strategies of Decentralisation on the Internet & Possible Countermeasures. *Institute for Strategic Dialogue (ISD)*. Available at: https://www.isdglobal.org/isd-publications/inside-the-digital-labyrinth/

22 Kinder-Kurlanda, K. E. and Weller, K. (2020). Perspective: Acknowledging Data Work in the Social Media Research Lifecycle. *Frontiers in Big Data*. Volume 3 – 2020. Available at: https://doi.org/10.3389/fdata.2020.509954

23 Hammer, D., Rübbert, Z. and Schwieter, C. (2022). In the blind spot – How right-wing extremists use alternative platforms for radicalisation. Conference report on the 2021 Annual Conference for the project »Countering Radicalisation in Right-Wing Extremist Online Subcultures«. *Institute for Strategic Dialogue (ISD)*. Available at: https://www.isdglobal.org/isd-publications/in-the-blind-spot-how-right-wing-extremists-use-alternative-platforms-for-radicalisation/

24 European Commission (2022). 2022 Strengthened Code of Practice on Disinformation. *European Commission*. Available at: https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation

25 Transparency Centre (2023). Reports Archive. Available at: https://disinfocode.eu/reports-archive/?years=2023

26 Google (2010). Greater transparency around government requests. *Official Blog*. Available at: https://googleblog.blogspot.com/2010/04/greater-transparency-around-government.html

27 The Santa Clara Principles On Transparency and Accountability in Content Moderation. Available at: https://santaclaraprinciples.org/

28 Singh, S. and Leila Doty, L. (2021). The Transparency Report Tracking Tool: How Internet Platforms Are Reporting on the Enforcement of Their Content Rules. *Open Technology Institute*. Available at: https://www.newamerica.org/oti/reports/transparency-report-tracking-tool/

29 Gleicher, N., Nimmo, B., Agranovich, D., and Dvilyanski, M. (2021). Adversarial Threat Report. Meta/Facebook. Available at: https://about.fb.com/wp-content/uploads/2021/12/Metas-Adversarial-Threat-Report.pdf

30 For example, *New America's Open Technology Institute* proposed Transparency Reporting Toolkits focused on government requests for user data as well as content takedown reporting. Similar efforts have been led by other relevant stakeholders, including Tech against Terrorism's Transparency reporting guidelines for governments or the Voluntary Transparency Reporting Framework developed by the Organisation for Economic Co-operation and Development (OECD).

31 European Commission (2023). Digital Services Act: Commission designates first set of Very Large Online Platforms and Search Engines. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413

32 Hansen Shapiro, E., Sugarman, M., Bermejo, F., and Zuckerman, E. (2021). New Approaches to Platform Data Research. *NetGain Partnership*. Available at: https://drive.google.com/file/d/1bPsMbaBXAROUYVesaN3dCtfaZpXZgI0x/view

33 Social Science One (2018). Public Launch. *Harvard's Institute for Quantitative Social Science*. Available at: https://socialscience.one/blog/social-science-one-public-launch

34 Schrage, E. and Ginsberg, D. (2018). Facebook Launches New Initiative to Help Scholars Assess Social Media's Impact on Elections. Facebook Newsroom. *Meta*. Available at: https://about.fb.com/news/2018/04/new-elections-initiative/

35 Social Science One (2018). Public Launch. *Harvard's Institute for Quantitative Social Science*. Available at: https://socialscience.one/blog/social-science-one-public-launch

[36] King, G. and Persily, N. (2020). A New Model for Industry–Academic Partnerships. *PS: Political Science & Politics*, 53(4), 703-709. doi:10.1017/S1049096519001021. Available at: https://www.cambridge.org/core/journals/ps-political-science-and-politics/article/new-model-for-industryacademic-partnerships/AD7D0B8EA582DC017D9A24754D833CAA

[37] King, G. and Persily, N. (2020). Unprecedented Facebook URLs Dataset now Available for Academic Research through Social Science One. *Harvard's Institute for Quantitative Social Science*. Available at: https://socialscience.one/blog/unprecedented-facebook-urls-dataset-now-available-research-through-social-science-one

[38] Ibid.

[39] Evans, G. and King, G. (2022). Statistically Valid Inferences from Differentially Private Data Releases, with Application to the Facebook URLs Dataset. Political Analysis, Pp. 1-21. Available at: https://tinyurl.com/yc5mx3sw; Evans, G. King, G., Schwenzfeier, M. and Thakurta, A. (2020). Statistically Valid Inferences from Privacy Protected Data. *American Political Science Review*. Available at: https://tinyurl.com/yd4xbnb8

[40] King, G. and Persily, N. (2020). Unprecedented Facebook URLs Dataset now Available for Academic Research through Social Science One. *Harvard's Institute for Quantitative Social Science*. Available at: https://socialscience.one/blog/unprecedented-facebook-urls-dataset-now-available-research-through-social-science-one

[41] Persily, N. (2022). Platform Transparency: Understanding the Impact of Social Media. Testimony Before the United States Senate Committee on the Judiciary – Subcommittee on Privacy, Technology, and the Law. Available at: https://www.judiciary.senate.gov/imo/media/doc/Persily%20Testimony.pdf

[42] Ibid.

[43] Vogus, C. (2023). Defending Data: Privacy Protection, Independent Researchers, and Access to Social Media Data in the US and EU. *Center for Democracy & Technology (CDT)*. Available at: https://cdt.org/wp-content/uploads/2023/01/2023-01-23-CDT-Defending-Data-Independent-Researcher-Access-to-Data-report-final.pdf

[44] Recital 47 of the GDPR refers to the "reasonable expectations of data subjects based on their relationship with the controller". See here: Proton AG (2023). What is GDPR, the EU's new data protection law?. GDRP.EU. Available at: https://gdpr.eu/what-is-gdpr/

[45] Article 40, Official Journal of the EU (2022). Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC (Digital Services Act). Volume 65. 27 October. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&from=EN

[46] Vermeulen, M. (2022). Researcher Access to Platform Data: European Developments. *Journal of Online Trust and Safety*. Vol. 1 No. 4 (2022). Available at: https://tsjournal.org/index.php/jots/article/view/84/31

[47] European Commission (2022). 2022 Strengthened Code of Practice on Disinformation. *European Commission*. Available at: https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation

[48] NYU Cybersecurity for Democracy (2022). Transparency For "Reasonably Public" Platform Content. Why we need transparency of certain types of public, high reach content. Policy Overview. *NYU Cybersecurity for Democracy*. Available at: https://cybersecurityfordemocracy.cdn.prismic.io/cybersecurityfordemocracy/532dcdca-27dc-478b-b579-411d82b7e903_20220505_C4D_HighEngagement_sum_v5.pdf

[49] Vermeulen, M. (2022). Researcher Access to Platform Data: European Developments. *Journal of Online Trust and Safety*. Vol. 1 No. 4 (2022). Available at: https://tsjournal.org/index.php/jots/article/view/84/31

[50] European Commission (2022). 2022 Strengthened Code of Practice on Disinformation. European Commission. Available at: https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation

[51] CrowdTangle (2023). What data is CrowdTangle tracking? Available at: https://help.crowdtangle.com/en/articles/1140930-what-data-is-crowdtangle-tracking

[52] Alba, D. (2022). Meta Pulls Support for Tool Used to Keep Misinformation in Check. *Bloomberg*. Available at: https://www.bloomberg.com/news/articles/2022-06-23/meta-pulls-support-for-tool-used-to-keep-misinformation-in-check?leadSource=uverify%20wall

[53] Roose, K. (2021). Inside Facebook's Data Wars. *New York Times*. Available at: https://www.nytimes.com/2021/07/14/technology/facebook-data.html

[54] Albert, J. (2022). Facebook's gutting of CrowdTangle: a step backward for platform transparency. *AlgorithmWatch*. Available at: https://algorithmwatch.org/en/crowdtangle-platform-transparency/

[55] Meta (2022). Widely Viewed Content Report: What People See on Facebook. Q4 2022 report. *Transparency Center*. Available at: https://transparency.fb.com/data/widely-viewed-content-report/

[56] Vogus, C. (2022). Improving Researcher Access to Digital Data. A Workshop Report. *Center for Democracy & Technology (CDT)*. Available at: https://cdt.org/wp-content/uploads/2022/08/2022-08-15-FX-RAtD-workshop-report-final-int.pdf

[57] Vogus, C. (2023). Defending Data: Privacy Protection, Independent Researchers, and Access to Social Media Data in the US and EU. *Center for Democracy & Technology (CDT)*. Available at: https://cdt.org/wp-content/uploads/2023/01/2023-01-23-CDT-Defending-Data-Independent-Researcher-Access-to-Data-report-final.pdf

[58] Mozilla (2021). YouTube Regrets. A crowdsourced investigation into YouTube's recommendation algorithm. *foundation.mozilla.org*. Available at: https://assets.mofoprod.net/network/documents/Mozilla_YouTube_Regrets_Report.pdf

[59] Ricks, B. and McCrosky, J. (2022). Does This Button Work? Investigating YouTube's ineffective user controls. *foundation.mozilla.org*. Available at: https://assets.mofoprod.net/network/documents/Mozilla-Report-YouTube-User-Controls.pdf

[60] Edelson, L. et al. (2021). Researchers, NYU, Knight Institute Condemn Facebook's Effort to Squelch Independent Research about Misinformation. Press Statement. *Knight First Amendment Institute*. Available at: https://knightcolumbia.org/content/researchers-nyu-knight-institute-condemn-facebooks-effort-to-squelch-independent-research-about-misinformation

[61] Erwin, M. (2021). Why Facebook's claims about the Ad Observer are wrong. *The Mozilla Blog*. Available at: https://blog.mozilla.org/en/mozilla/news/why-facebooks-claims-about-the-ad-observer-are-wrong/

[62] Coons, C. (2022). Senator Coons, colleagues introduce legislation to provide public with transparency of social media platforms. *Press Release*. Available at: https://www.coons.senate.gov/news/press-releases/senator-coons-colleagues-introduce-legislation-to-provide-public-with-transparency-of-social-media-platforms

[63] Vogus, C. (2022). Improving Researcher Access to Digital Data. A Workshop Report. *Center for Democracy & Technology (CDT)*. Available at: https://cdt.org/wp-content/uploads/2022/08/2022-08-15-FX-RAtD-workshop-report-final-int.pdf

[64] Mozilla. Available at: https://blog.mozilla.org/security/2018/08/01/safe-harbor-for-security-bug-bounty-participants/

[65] The Code considers "Disinformation" to include "misinformation", "disinformation", "information influence operations", and "foreign interference in the information space", which are defined in the European Commission's Communication on the European Democracy Action Plan, p.18. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0790&from=EN

[66] Transparency Centre (2023). Available at: https://disinfocode.eu/

[67] Proton AG (2023). What is GDPR, the EU's new data protection law?. *GDRP.EU*. Available at: https://gdpr.eu/what-is-gdpr/

[68] EDMO (2022). Report of the European Digital Media Observatory's Working Group on Platform-to-Researcher Data Access. *European Digital Media Observatory (EDMO)*. Available at: https://edmoprod.wpengine.com/wp-content/uploads/2022/02/Report-of-the-European-Digital-Media-Observatorys-Working-Group-on-Platform-to-Researcher-Data-Access-2022.pdf

[69] In response to a call for comments from interested stakeholders in November 2020, tech companies submitted comments on EDMO's intention to launch a Working Group on 'Access to Data Held by Digital Platforms for the Purposes of Social Scientific Research.' See, for example, Meta's comments here: Available at: https://about.fb.com/wp-content/uploads/2020/12/Facebook-Response-to-EDMO-Request-for-Submissions.pdf

[70] Available at: EDMO (2022). Report of the European Digital Media Observatory's Working Group on Platform-to-Researcher Data Access. *European Digital Media Observatory (EDMO)*. Available at: https://edmoprod.wpengine.com/wp-content/uploads/2022/02/Report-of-the-European-Digital-Media-Observatorys-Working-Group-on-Platform-to-Researcher-Data-Access-2022.pdf

[71] Ibid.

[72] EDPS (2020). A Preliminary Opinion on data protection and scientific research. *European Data Protection Supervisor (EDPS)*. Available at: https://edps.europa.eu/sites/default/files/publication/20-01-06_opinion_research_en.pdf

[73] EDMO (2022). Report of the European Digital Media Observatory's Working Group on Platform-to-Researcher Data Access. *European Digital Media Observatory (EDMO)*. Available at: https://edmoprod.wpengine.com/wp-content/uploads/2022/02/Report-of-the-European-Digital-Media-Observatorys-Working-Group-on-Platform-to-Researcher-Data-Access-2022.pdf

74 Official Journal of the EU (2022). Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC (Digital Services Act). Volume 65. 27 October. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065&from=EN

75 Vermeulen, M. (2022). Researcher Access to Platform Data: European Developments. *Journal of Online Trust and Safety.* Vol. 1 No. 4 (2022). Available at: https://tsjournal.org/index.php/jots/article/view/84/31

76 Schwieter, C. (2022). Online Crisis Protocols – Expanding the Regulatory Toolbox to Safeguard Democracy During Crises. *Institute for Strategic Dialogue (ISD)*. Available at: https://www.isdglobal.org/isd-publications/online-crisis-protocols-expanding-the-regulatory-toolbox-to-safeguard-democracy-during-crises/

77 EDMO (2022). Report of the European Digital Media Observatory's Working Group on Platform-to-Researcher Data Access. *European Digital Media Observatory (EDMO)*. Available at: https://edmoprod.wpengine.com/wp-content/uploads/2022/02/Report-of-the-European-Digital-Media-Observatorys-Working-Group-on-Platform-to-Researcher-Data-Access-2022.pdf

78 Vermeulen, M. (2022). Researcher Access to Platform Data: European Developments. *Journal of Online Trust and Safety.* Vol. 1 No. 4 (2022). Available at: https://tsjournal.org/index.php/jots/article/view/84/31

79 Jaursch, J. (2022). Barriers to Strong DSA Enforcement – and How to Overcome Them. *Tech Policy Press*. Available at: https://techpolicy.press/barriers-to-strong-dsa-enforcement-and-how-to-overcome-them/

80 Jaursch, J. (2022). Platform oversight. Here is what a strong Digital Services Coordinator should look like. *Verfassungsblog*. Available at: https://verfassungsblog.de/dsa-dsc/

ISD | Institute for Strategic Dialogue

Amman | Berlin | London | Paris | Washington DC

www.isdgermany.org

Sponsored by:

Federal Foreign Office