Digital Policy Lab

Policy Digest #15

7 May 2024

Policy Digests offer an overview of recent digital policy developments in Digital Policy Lab (DPL) member countries, including regulatory and non-regulatory initiatives aiming to combat online harms such as disinformation, hate speech, extremist or terrorist content. In addition to general updates, each Policy Digest provides a snapshot of topic-specific schemes relevant to the upcoming DPL session.[1]

Section 1 Digital policy developments

Australia: Federal Court grants interim injunction requiring X to hide extreme violent content

Type Regulatory (enforcement action)
Status Ongoing

On 24 April 2024, the Australian Federal Court extended an interim injunction requiring X to hide video content of the alleged terrorist attack in Sydney on 15 April. The injunction followed Class 1 removal requests from eSafety to both Meta and X on 16 April, which Meta complied with. However, eSafety was unsatisfied with X's compliance actions and sought an interim injunction, leading to two hearings thus far. eSafety may issue removal notices under the 2021 Online Safety Act. The Act empowers the courts to issue civil penalties to corporations of up to $782 500 AUD per day for non-compliance with removal notices.

A final hearing is yet to be scheduled, where eSafety is expected to seek a permanent injunction and penalties against X. The extended interim injunction is valid until 10 May.

Canada: Online Harms Act (Bill C-63) proposed

Type Legislative
Status Proposal

On 26 February 2024, the Government of Canada tabled Bill C-63, which introduces a new Online Harms Act. The proposed Act imposes new duties on online platforms in Canada to act responsibly, protect children, and make certain content inaccessible. The Bill targets seven types of harmful content: content that sexually victimises a child or revictimises a survivor; intimate content communicated without consent; content used to bully a child; content that induces a child to harm themselves; content that foments hatred; content that incites violence; and content that incites violent extremism or terrorism. The Bill imposes no duties to proactively search for harmful content, but rather strict obligations following user reporting, with an exception for means to prevent the uploading of material that sexually victimises a child or revictimises a survivor.

In terms of structural changes, the Bill establishes a new digital safety regulator (Digital Safety Commission) and Digital Safety Ombudsperson to advocate for users and victims. It also proposes changes to the Canadian Criminal Code and Human Rights Act on hate speech and hate crimes, and amends existing online child sexual abuse legislation.

The Bill further introduces mechanisms for platform data access for research on online harms. While the details of data access provisions will depend on later regulations, the Bill opens accreditation eligibility for data access to those conducting

[1] We welcome any feedback from DPL members regarding additional developments, as well as own submissions from DPL members who wish to be featured in the digest.

education, advocacy, or awareness activities on online harms, as well as independent researchers. The newly established Digital Safety Commission is authorised to grant this accreditation to inventories of electronic data and to the electronic data of operators of social media services.

European Union & United States: Trade and Technology Council holds sixth ministerial meeting

Type Intergovernmental meeting
Status Published

On 4-5 April 2024, the EU and US met for the sixth ministerial-level meeting of the Trade and Technology Council (TTC). The meeting led to agreement on a range of digital policy issues. Ministers announced a new Dialogue between the EU Artificial Intelligence Office and the US Artificial Intelligence Safety Institute, as well as a reaffirmation of both parties' commitments to a risk-based approach to AI policy.

The meeting also produced a set of Joint Principles on combatting technology-facilitated gender-based violence (TFGBV). The Joint Principles included recommendations for online platforms to effectively address TFGBV and reiterated the importance of facilitating data access for research on the risks of TFGBV on online platforms.

Another relevant output from the meeting was a set of joint Recommended Actions for online platforms to protect defenders of human rights online. Ministers also committed to facilitating data access from online platforms and published a Status Report on platform mechanisms for researcher data access, including access to advertisement repositories; the findings of the Status Report are detailed in Part 2 of this Digest.

European Union: European Commission opens formal proceedings against Meta, TikTok, and AliExpress under the Digital Services Act (DSA)

Type Regulatory (enforcement)
Status Investigation proceedings initiated

On 30 April 2024, the European Commission opened formal proceedings against Meta for potential breaches of the DSA through Facebook and Instagram. The proceedings cover a range of areas, many being particularly salient in the lead-up to the June European Parliament elections. The Commission will investigate Meta's measures to address the dissemination of deceptive advertisements, disinformation campaigns and coordinated inauthentic behaviour in the EU; the role of Meta's recommender systems in promoting political content; and the possible inefficacy and noncompliance of its mechanisms to flag illegal content. The lack of an effective "real-time civic discourse and election-monitoring tool" available to third parties, following Meta's deprecation and planned withdrawal of the CrowdTangle platform, is also under investigation. The Commission suspects that the unavailability of CrowdTangle or a viable replacement has resulted in a failure to assess and adequately mitigate Facebook and Instagram's risks to civic discourse and electoral processes; this is especially a concern in the lead-up to the June European Elections, as well as those in other member states.

On 22 April 2024, the European Commission announced its second proceedings against TikTok for potentially breaching DSA regulations with the launch of TikTok Lite in France and Spain. The concerned DSA provision is the requirement for Very Large Online Platforms (VLOPs) and Search Engines (VLOSEs) to submit risk assessment reports, including mitigation measures for systemic risks, prior to launching new features. TikTok Lite's "Task and Reward Program" introduces a point system for engaging with content, following accounts or inviting new users in exchange for coins or gift cards. The Commission is

concerned about the addictiveness of this design, particularly in view of TikTok's young user base. The lack of effective age verification and addictive functionalities are also under investigation in the first formal proceedings launched against TikTok under the DSA in February 2024, along with data access for researchers and advertising transparency. This paves the way for further enforcement steps by the Commission which, in the recent case, includes the possibility of shutting down "Lite" in the EU as an interim measure until its safety is determined. On 24 April, TikTok voluntarily suspended the program.

On 14 March 2024, the European Commission initiated proceedings against AliExpress. Areas of concern are risk assessment and mitigation regarding illegal content and consumer protection, content moderation and the internal complaint-handling system, advertising and algorithm transparency, data access for researchers, and traceability of traders.

European Union: European Commission sends letters of formal notice to several member states to designate Digital Services Coordinators (DSCs) under the DSA

Type Regulatory (implementation and enforcement)
Status Formal notices sent

On 24 April 2024, the European Commission declared that it had sent letters of formal notice to those member states yet to designate a DSC under the DSA, as well as those yet to give their DSCs sufficient mandates to fulfil their duties. Member states were due to determine the competent authorities to act as their respective DSCs by 17 February 2024, the date the DSA entered fully into force for all services. Estonia, Poland, and Slovakia have not done so yet; Cyprus, the Czech Republic and Portugal "still have to empower them with the necessary powers and competences to carry out their tasks, including the imposition of sanctions." Other key DSC tasks include vetting researchers for data access, determining trusted flaggers and receiving user complaints. The six states have two months to respond before the Commission may issue reasoned opinions, explaining what it regards as an infringement and warning to resolve the issue, or else it can bring a proceeding before the Court of Justice of the European Union (CJEU).

European Union: European Commission opens consultation on the evaluation of the Terrorist Content Online Regulation

Type Regulatory (consultation)
Status Consultation open

On 11 April 2024, the European Commission announced the opening of a consultation to evaluate the Terrorist Content Online Regulation ('TCO,' Regulation 2021/783). It seeks to inquire into the regulation's "relevance, effectiveness, efficiency, coherence and EU added value". The TCO aims to curb the spread of terrorist content online to disrupt digital radicalisation and recruitment strategies. The consultation is open until 9 May 2024. Responses will be used for reporting on the implementation of the regulation, with adoption by the Commission planned for the second quarter of 2025.

European Union: Interim measures for online child sexual abuse material prolonged, new compromise text drafted

Type Legislative (compromise text for draft law)
Status Passed European Parliament / in negotiations

On 10 April 2024, the European Parliament passed the Regulation on the Extension of Derogation from the ePrivacy Directive, thereby prolonging an interim measure to detect and prevent online child sexual abuse material (CSAM) until April 2026 while a new draft law on this issue is negotiated.

According to Euractiv, the latest compromise text by the Belgian EU Council Presidency for the new regulation on detecting and preventing online CSAM, dated 9 April, elaborates on provider risk category indicators and companies' data retention duties. Previous drafts were criticised over privacy concerns vis-à-vis judicial requests to scan private messaging services and age verification measures. The text clarifies reporting obligations after detection orders and foresees voluntary flagging by online services to a Coordinating Authority in each member state over suspicions regarding users with repeated behaviours. The Coordinating Authority would also oversee redress requests and risk assessment and mitigation reports. The new law also aims to create a new EU Centre for Child Protection to conduct audits, advise on detection technologies, support victims, and cooperate with Europol.

France: National Assembly approves new online safety legislation and officially designates Arcom as DSC

Type Legislative
Status Undergoing review by Constitutional Council

On 10 April 2024, the French National Assembly approved a new, wide-ranging digital policy bill after months of negotiations. The *Sécuriser et regular l'espace numérique* (SREN) bill transposes major EU legislation, including the DSA and the Digital Markets Act (DMA), into national law, and officially designates Arcom as the national DSC. The Bill also introduces additional online safety and digital markets laws.

Particularly relevant are strengthened penalties regarding online hate and harassment, which may now result in court-imposed bans from social media sites for up to a year, as well as fines for platform non-compliance (EUR 75 000 per account). The Bill further creates a new online contempt offence designed to punish harassment and discriminatory content online, with convicted individuals liable for fines of up to EUR 300. Arcom is also empowered to order news operators to stop broadcasting foreign propaganda material subject to European sanctions.

In addition to changes to offences and penalties, the Bill also introduces programmes designed to improve youth literacy regarding abuses linked to AI-generated content, parents' understanding of online harms, and students' awareness of online gender-based and sexual violence.

The Bill is currently under consideration by the French Constitutional Council following referrals from the *Rassemblement national* and *La France insoumise* parties over criticisms of its constitutionality.

Germany: Ministry of the Interior presents measure package to combat right-wing extremism

Type Non-legislative
Status New measures presented

On 13 February 2024, the German Ministry of the Interior (BMI) adopted new measures to combat right-wing extremism, including hate and right-wing extremist content online. The Central Reporting Office for Illegal Content on the Internet at the Federal Criminal Police Office (ZMI BKA) is to be further expanded. Generally, the Federal Criminal Police Office is adapting its strategies to prosecute online crimes. Additionally, platforms are to remove right-wing extremist content online more efficiently. The Federal Office for the Protection of the Constitution (BfV) is to monitor developments on coordinated influence campaigns and disinformation and take countermeasures. Similarly, the Ministry of the Interior is building a new early detection unit for the government to identify foreign manipulation and influence campaigns.

Italy: Competition Authority AGCM imposes EUR 10 million fine on TikTok over alleged failure to remove dangerous content

Type Regulatory (enforcement)
Status Fine imposed

On 6 March 2024, the Italian Competition Authority (AGCM) imposed a EUR 10 million fine on TikTok for failing to take appropriate measures against the spread of content it classified as dangerous for minors. An example for content the AGCM deems harmful is the "French scar" challenge which requests users to pinch their cheeks until a lasting bruise appears. The regulator reasons that TikTok does not take into account how vulnerable groups have a tendency to copy other people's behaviour.

United Kingdom: Ofcom publishes principles for best practice for media literacy by design

Type Regulatory
Status Published

On 19 April 2024, Ofcom published its Best-Practice Principles on media literacy in platform design, as well as a summary of stakeholder responses to the autumn 2023 consultation on the Principles. Best practices highlighted in the Principles include proactivity, priority, transparency, and accountability, such as creating media literacy by design policies and on-platform interventions; user-centric design and timely interventions, such as designing feedback to users to increase literacy; and monitoring and evaluating, such as establishing literacy outcomes and indicators. Ofcom's work on media literacy is related to, but distinct from, its duties under the Online Safety Act (OSA). Unlike the OSA codes of practice, the Principles are non-binding and voluntary.

United Kingdom: Criminal Justice Bill to be amended to criminalise creation of sexually explicit deepfakes

Type Legislative
Status Under deliberation

On 16 April 2024, the UK government announced that it will amend the Criminal Justice Bill to criminalise the creation of sexually explicit deepfakes without consent. According to the new law, perpetrators will be prosecuted and face a criminal record as well as an unlimited fine, regardless of an intent to share the created content. The intent to cause humiliation or distress to the depicted person is sufficient. If it is still shared after the prosecution for its creation, imprisonment is possible. This development is part of a government programme of measures to better protect women and girls, especially online, following the passing of the OSA, which first criminalised sharing sexually explicit deepfakes without consent.

United Kingdom: Ofcom issues call for evidence on categorisation of services under Online Safety Act, publishes advice to Government on categorisation thresholds

Type Regulatory
Status Under deliberation

On 25 March 2024, Ofcom opened a call for evidence on additional duties for categorised services under the OSA. According to the OSA, all in-scope technology firms must have appropriate safety provisions and categorised services are subject to a series of additional requirements. These requirements vary depending on the category and include greater user control over what content they see, protections for news publishers and journalistic content, and transparency reports.

Ofcom also concurrently published its advice to the UK Secretary of State on the thresholds for categorising services. The recommendations – based on research conducted by Ofcom – define the thresholds for Categories 1, 2A, or 2B based on several functionalities and characteristics, including the size of a services' user base, the presence of content recommendation systems, and users' abilities to send direct messages or forward/reshare user-generated content.

The Secretary of State will consider Ofcom's advice as part of determining category thresholds, which will be set in secondary legislation. Ofcom will be responsible for enforcing duties of categorised services and aims to publish draft proposals regarding the additional duties on these services in early 2025. It is also expected to launch a formal consultation on duties for categorised services in 2025 and will account for responses to the call for evidence, which closes on 20 May.

United Kingdom: Data Protection and Digital Information Bill passes to Committee Stage with proposed data access amendments

Type Legislative
Status Under deliberation

On 20 March 2024, the Data Protection and Digital Information Bill entered Committee Stage in the UK House of Lords. The Bill includes provisions on information and data processing and sharing, privacy, and data use by public services, and reforms the information regulator. Proposed amendments on data access were also made during the Bill's second reading in the Lords on 19 December 2023. Modelled after provisions in the DSA, the proposed data access provisions would introduce a duty for regulated platforms to enable data and information access to approved independent researchers under certain conditions. Researchers would be able to access data for the sole purpose of research that "contributes to the detection, identification and understanding of systemic risks of non-compliance" with UK law upheld by one or more regulatory bodies (the Information Commissioner, Competition and Markets Authority, Office of Communications, and the Financial Conduct Authority). The bill will then pass to the report stage in Lords.

United States: 21st Century Peace Through Strength Act signed by President Biden

Type Legislative
Status In force

On 24 April 2024, US President Biden signed the 21st Century Peace Through Strength Act as part of a larger piece of foreign aid legislation. Notably, the package included the Protecting Americans From Foreign Adversary Controlled Applications Act, colloquially known as the "TikTok Ban," which prohibits the distribution, maintenance, or updating of any applications in the US that are controlled by foreign adversaries. Foreign adversaries are defined by covered nations named in 4872(d)(2) of title 10 of the United States Code, which currently include North Korea, China, Russia, and Iran. The Bill specifically names applications run by ByteDance and TikTok as foreign adversary-controlled applications. ByteDance, per the Bill's enactment, now has 270 days to divest ownership of TikTok or cease its operations in the US. It is expected that ByteDance will fight this decision in the courts.

Section 2 Topic-specific snapshot: "Reviewing Developments on Access to Platform Data for Independent Researchers"

This section provides an overview of how data access for independent researchers is covered by two key pieces of online safety legislation: the EU Digital Services Act (DSA) and the proposed Canadian Online Harms Act (Bill C-63). It also summarises selected analyses and recommendations published by government agencies and civil society organisations on data access for independent researchers, as well as developments in private sector approaches to data access.

Regulatory Refresher: Data Access in the EU Digital Services Act and Canada's proposed Online Harms Act

The EU's DSA introduces a provision for data access and scrutiny on very large online platforms (VLOPs) and search engines (VLOSEs) under certain conditions in Article 40.

- Art. 40.1 provides data access for regulators, the Digital Services Coordinator of establishment (DSCe) and the European Commission, for the purpose of monitoring and assessing DSA compliance.

- Art. 40.4 provides access to vetted researchers via the DSCe. DSCes are responsible for vetting researchers, and criteria for vetted researchers are specified in Art. 40.8. They must be affiliated to a research organisation, independent from commercial interests, disclose their funding and publish results. Research must be done on "systemic risks" (Art. 34.1) in the EU and digital services' mitigation measures (Art. 35). DSCes submit research requests to platforms on behalf of the vetted researchers. Platforms have a right to ask the DSCe to amend data access requests if they lack the data or if vulnerable information such as trade secrets are affected (Art. 40.5). The European Commission is expected to release a delegated act on data access for vetted researchers imminently, which may provide further details.

- Art. 40.12 provides access to public data. This also includes non-profit organisations that fulfil key requirements in Art. 40.8. This may include civil society at large, including journalists. Access should be given, ideally in real time, via an online tool. A similar clause can be found in the EU's Code of Practice on Disinformation.

Canada's proposed Online Harms Act (Bill C-63) authorises the Digital Safety Commission of Canada, a newly proposed regulator in the Bill, to accredit certain persons conducting education, advocacy, awareness, or research activities on online harms related to the purposes of the Act (section 73). Accredited persons may access inventories and electronic data included in the digital safety plans submitted to the Commission by regulated services, a category which will be defined in later regulation. In terms of categorisation, it is worth noting that the Act in its current form allows the Governor in Council to designate particular services as regulated if they are satisfied that there is a significant risk that harmful content is accessible on the service. This will potentially allow for access to data on smaller but high-risk platforms, which is not possible under the EU's DSA. Information accessible through digital safety plans includes: information on compliance with services' duties to mitigate risks of exposure to harmful content and implement risk mitigation measures; compliance on age-appropriate design, including a description of integrated design features; measures implemented to protect children; resources allocated to comply with duties introduced under the Act; granular and quantitative details on content moderation; and topics and summaries of the findings of any research conducted by or on behalf of the operator relating to harmful content on the service, content that poses a risk of significant psychological or physical harm, or design features that pose a risk of significant psychological or physical harm.

Platform Approaches to Data Access in 2024

This section provides a brief summary of selected platform policies on data access, with a focus on recent notable changes to data access policies. The following list, current at the timing of writing, summarises these approaches.

Notably, on 18 January 2024, the European Commission sent requests for information regarding research access to publicly available data to 17 Very Large Online Platforms and Search Engines under the DSA. Platforms subject to requests included Facebook, Instagram, TikTok, and YouTube.

- On 14 March 2024, Meta-owned CrowdTangle, the Application Programming Interface (API) used to analyse Facebook and Instagram content, announced that it will terminate its operations on 14 August 2024. While the company points to the Meta Content Library and Content Library API as an adequate replacement, researchers and media outlets argue that the functionalities and granularities of data differ greatly between the tools, thus making them incomparable. Moreover, journalists do not have access to the Content Library. The decision to close down CrowdTangle was preceded by hints as AlgorithmWatch chronicled in 2022: the API was no longer updated, new user requests were not processed, and resources were cut over time. Meta also seemingly shut down independent research projects such as the NYU Ad Observatory. Nevertheless, the announcement in March was met with protest by civil society, including an open letter initiated by the Mozilla Foundation, calling for the tool to be kept in place. On 30 April 2024, the European Commission opened formal proceedings against Meta, also regarding the "non-availability of an effective third-party real-time civic discourse and election-monitoring tool ahead of the upcoming elections to the European Parliament."

- On 20 July 2023, TikTok announced the expansion of its research API to Europe, following an initial US launch earlier in 2023. This expansion proceeded TikTok's obligations to provide data access to independent researchers under the DSA. The TikTok research API is available free of charge for non-profit researchers, following an initial application. TikTok also allows access to its Commercial Content Library, which provides access to a searchable database of paid advertising and commercial content on TikTok. TikTok's suspected shortcomings in providing researchers access to TikTok's publicly accessible data, as mandated under Article 40 of the DSA, is also under investigation.

- On 9 February 2023, X closed free access to its API, which until then was widely used for collecting platform data for public-interest research. This was shortly followed by the launch of paid data access tiers in March 2023, with researchers reporting access costs of up to and beyond USD 42,000 per month. These costs are prohibitive to many researchers at academic institutions, media companies, or civil society organisations, and have been criticised heavily by those conducting public-interest research. Since November 2023, limited free access has ostensibly been available to vetted researchers on topics that contribute to "the detection, identification and understanding of systemic risks in the European Union and only to the extent necessary for X to comply with its obligations under the DSA." However, concerns that X continues to provide inadequate access to data have continued, leading to the European Commission opening formal proceedings against X for potential noncompliance with the DSA. However, for public interest research outside of the thematic or geographic scope of the DSA, data access to X is a growing challenge.

- On 12 July 2022, YouTube's Researcher Programme was launched for researchers affiliated with higher-learning institutions. This launch proceeded YouTube's obligations to provide data access to independent researchers under the DSA. The Programme requires an eligibility check for "scaled, expanded access to global video metadata across the entire public YouTube corpus" via YouTube's Data API. Next, researchers must create an API project in Google Cloud and send in an application. Researchers had long lobbied for meaningful data access to enable public-interest research on YouTube, as its API was criticised for lacking relevant data to study the algorithm, setting rate limits, and not providing alternative audit

tools for researchers to assess online threats. As a result, researchers had previously mainly resorted to data scraping and donations. In 2023, the Researcher Programme was criticised for its narrow definition of eligible researchers, for not allowing third-party data sharing and mandating the disclosure of government data sharing and advance notices of research publications. Moreover, the Mozilla Foundation noted that the only significant difference to the previous public API are higher rate limits on a case-by-case basis – available data did not significantly change.

Further Reading: Data Access Analyses and Recommendations

Enabling Research with Publicly Accessible Platform Data: Early DSA Compliance Issues and Suggestions for Improvement, *Weizenbaum Institute et al.,* 2024

The Weizenbaum Institute, the European New School of Digital Studies and Stiftung Neue Verantwortung published a position paper as an early assessment of DSA compliance issues regarding publicly accessible platform data. This is covered by Art. 40.12, which asks VLOPs and VLOSEs to provide publicly accessible data to researchers that meet a certain set of criteria. The authors find that while some platforms did implement this requirement at least partially, there are "serious concerns" regarding full DSA compliance. They also point to the European Commission's formal request of information from 17 VLOPs and VLOSEs to elaborate on their compliance with this provision as proof.

Furthermore, the paper describes independent researchers challenges in requesting publicly accessible data in order to inform both the European Commission as well as Digital Services Coordinators (DSCs) to fulfil their duties as the DSA's overseeing entities. Lastly, the paper provides recommendations on how to reach compliance, based on exchanges with peers and the DSA 40 Data Access Tracker. This includes easy-to-find application forms, wider interpretation of eligibility criteria and adequate research questions, quicker responses with elaborations for the grounds of rejection, documentation of accessible data by platforms, fewer restrictions on data access once a request has been granted, an end to pre-publication reviews and continued pre-DSA access modes.

Got Complaints? Want Data? Digital Service Coordinators will have your back – or will they?, *AlgorithmWatch,* 2024

In a blogpost from 14 February 2024, AlgorithmWatch outlines how the shutdown of CrowdTangle and X's new charges for data access burdens independent researchers in their vital task of understanding and assessing risks on online platforms. Regarding publicly accessible data, AlgorithmWatch stresses the dire need for analytical tools and interfaces to conduct effective and efficient research. The DSA promises improvements on paper, yet implementation and enforcement is only fully starting now. The piece specifically asks the question of whether the DSCs in each member state will actually help researchers by timely and appropriately responding to vetting and non-public data access requests, transferring them to the platforms and judging platform's amendment requests in a way that eases the pressures that exist. Moreover, at the time of writing the DSA still lacks clarity in many aspects, several DSCs are not yet set up sufficiently, and key upcoming elections require urgent data access for proper investigations into online harms. AlgorithmWatch was among the first organisations to request platform data under the DSA when it fully went into force by submitting a request to access Microsoft data.

Policy Approaches to Addressing Data Access Challenges in the Evolving Online Ecosystem,
Institute for Strategic Dialogue, Digital Policy Lab, 2023

This policy brief from the Digital Policy Lab summarises key findings from an 18-month research project on online harms on small and medium-sized platforms. It provides an overview of key findings from the research, with a focus on data access challenges present when researching hate, extremism, and disinformation on the platforms Telegram, Discord, and Odysee. The brief also provides an overview of existing or proposed legislation in key jurisdictions, including the EU, US, UK, Australia, New Zealand and Canada, assessing the extent to which they would impact access to data for researchers from smaller or medium-sized platforms. It concludes with a series of recommendations for the private sector, policymakers, and the research community to address the data access challenges identified related to smaller and medium-sized platforms. The brief's focus on small and medium-sized platforms reveals the limitations of regulatory approaches to data access, such as the DSA, that primarily or entirely focus on data access to large platforms. While other elements of the data access policy and advocacy have since developed further, the brief's observations regarding smaller platforms remain relevant.

Status Report: Mechanisms for Researcher Access to Online Platform Data,
Trade and Technology Council, 2024

This technical report from the sixth ministerial meeting of the EU-US Trade and Technology Council provides an overview of mechanisms for academic and civil society access to online platform data. It summarises mechanisms available to researchers in the EU and/or US, largely through VLOP and VLOSE measures to comply with the DSA. Mechanisms are described and compared across a range of elements, including access methods, data availability, rate limits, access conditions (e.g., research qualifications, geographic location), and terms of agreement (e.g., prepublication review, open access publications). The report also compares advertisement repositories against the same set of elements. The appendix to the report provides a useful comparative overview of data access programs in a table format and includes comparisons of interface design, access criteria, application requirements, and availability of data dictionaries or documentation.

Policy Is Urgently Necessary to Enable Social Media Research,
Tech Policy Press (2023) article by Dylan Baker, Research Engineer at the Distributed AI Research Institute & Public Voices Fellow on Technology in the Public Interest with The OpEd Project, in partnership with The MacArthur Foundation

In a piece from late December 2023, US-based researcher Dylan Baker calls for effective legislation in the United States to make sure it is possible to conduct public interest research on social media platforms. Pointing out surging information warfare in the context of the Israel-Gaza conflict, Baker underlines the necessity of allowing research into online threats amid the massive amounts of content uploaded daily, as well as companies' and politicians' increasing

campaigns against researchers. The author refers to Elon Musk's lawsuits against researchers over advertiser losses and Republican politicians' adversarial actions against researchers from universities and think tanks to underline that the lead-up to 2024's elections has intensified pressures on public interest research. Baker further criticises hurdles such as regional restrictions and lengthy application procedures for API access which platforms control. Once access is granted, data is often incomplete or gets withdrawn, which leads researchers to opt for data scraping and approaches that may break Terms of Services. The author calls for a third-party entity in the US to grant data access with the power to fine platforms for non-compliance.

About the Digital Policy Lab
The Digital Policy Lab (DPL) is an inter-governmental working group focused on charting the regulatory and policy path forward to prevent and counter disinformation, hate speech, extremism and terrorism online. It is comprised of a core group of senior representatives of relevant ministries and regulators from key liberal democratic countries. The DPL aims to foster inter-governmental exchange, provide policymakers with access to sector-leading expertise and research, and build an international community of policy practice around key regulatory challenges in the digital policy space. We thank the Alfred Landecker Foundation for their support for this project.