Digital Policy Lab

Policy Digest #6

31 August 2022

ISD Powering solutions to extremism, hate and disinformation

Sponsored by Federal Republic of Germany Foreign Office

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: Basic Online Safety Expectations and Digital Platform Regulators Forum

Type Regulatory guidance
Status Published

On 24 July 2022, the eSafety Commissioner published new guidance for members of the general public, industry and other stakeholders about the Basic Online Safety Expectations set out in the Online Safety Act of 2021. The guidance provides advice for service providers on implementation and responding to requests for information, notices or determinations, outlines how the eSafety Commissioner will approach compliance and enforcement, and sets out the rights of providers to seek reviews of eSafety Commissioner decisions. The guidance is non-binding, but does outline the powers of the eSafety Commissioner to require reporting from individual companies, or specific types of providers, and issue public statements of assessing (non-)compliance.

On 28 June 2022, the Digital Platform Regulators Forum (DP-REG), which includes the Australian Competition and Consumer Commission (ACCC), Australian Media and Communications Authority (ACMA), eSafety Commissioner (eSafety) and Office of the Australian Information Commissioner (OAIC), further agreed on a collective set of priorities for 2022/23. The forum's strategic priorities for 2022/23 include a focus on the impact of algorithms, seeking to increase transparency of digital platforms' activities and how they are protecting users from potential harm, and increased collaboration and capacity building between the four members. According to the forum's Terms of Reference, a 'digital platform' includes, but is not limited to, "internet search engines, digital content aggregators, social media services, private messaging services, media referral services and electronic marketplaces". The forum's activities and outputs include enhancing "regulatory capabilities across the DP-REG".

Canada: The Online Streaming Act (Bill C-11)

Type Regulatory
Status Passed in the House of Commons

On 21 June 2022, Canada's House of Commons passed Bill C-11, also known as the Online Streaming Act, amending the Broadcasting Act, which sets out the broadcasting policy for Canada, and the role and powers of the Canadian Radio-television and Telecommunications Commission (CRTC). The Bill adds "online undertakings", defined as "undertaking for the transmission or retransmission of programs over the Internet for reception by the public" as a distinct class of broadcasting undertakings. This would include any platform airing programmes on the internet in Canada, from streaming services like Netflix and Spotify to YouTube and TikTok. The Bill "encourage[s] the development of Canadian expression by providing a wide range of programming that reflects Canadian attitudes, opinions, ideas, values and artistic creativity, by displaying Canadian talent in entertainment programming and by offering information and analysis concerning Canada and other countries from a Canadian point of view, and foster an environment that encourages the development and export of Canadian programs globally".

[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.

After passing through the Heritage Committee and House of Commons, the Senate is expected to address remaining issues, especially the criticised ambiguity in defining which content will be considered "Canadian", over the coming review in autumn 2022.

EU: Digital Services Act (DSA) and Digital Markets Act (DMA)

Type Regulatory (legislative acts)
Status Approved

On 4 July 2022, the European Parliament held the final vote on the Digital Services Act (DSA) and Digital Markets Act (DMA). On 18 July, the Council gave its final approval of the DMA on new rules for a fair and competitive digital sector. The Act aims to ensure a digital level playing field that establishes clear rights and rules for large online platforms ('gatekeepers'). Among other obligations, gatekeepers will have to notify the European Commission about their intent to merge or acquire another company providing "core platform services" or other digital services. The DMA will start to apply six months following its entry into force. The gatekeepers will have a maximum of six months after they have been designated to comply with the new obligations. The DSA is expected to be adopted by the Council in September 2022.

On 5 July 2022, the European Commission published a short blog post from Commissioner Breton outlining the Commission's plans for enforcing both the DSA and DMA. This includes establishing expert teams in DG Connect focused on societal, technical and economic issues, adding specific expertise on data science and algorithmic systems, and creating a European Centre for Algorithmic Transparency. These will cooperate with DG Competition, the Commission Legal Service and the EC Joint Research Centre, as well as national regulators in each EU Member State.

Ireland: Online Safety and Media Regulation (OSMR) Bill

Type Regulatory
Status Seanad Report Stage

On 11 July 2022, the Minister for Tourism, Culture, Arts, Gaeltacht, Sport and Media, Catherine Martin, tabled amendments to the Online Safety and Media Regulation (OSMR) Bill. Their primary purpose is to address issues raised by Senators during Seanad Committee Stage, which concluded on 31 May 2022. The amendments require that at least one of the commissioners within the newly established regulator, "Coimisiún na Meán (the Media Commission)", will be explicitly designated as an "Online Safety Commissioner".

UK: Online Safety Bill (OSB)

Type Non-regulatory
Status Committee report stage

On 12 July 2022, the Online Safety Bill completed its Commons Report stage, which gives MPs an opportunity to consider further amendments. The debate continued to demonstrate broad overall cross-party support for the Bill. However, concerns were raised in a number of areas, including the powers given to the Secretary of State and their impact on the independence of Ofcom, the lack of specific provisions to address online violence against women and girls, and the lack of clarity around both the platforms and specific harms in scope.

The Bill's progress through parliament has been delayed due to the Conservative Party's leadership election contest. The Bill is expected to return in September once a new Prime Minister is selected and a new Cabinet is in place, but could be further delayed if the new Prime Minister or DCMS Minister decide to review the current draft and/or make any significant changes. Both of the two remaining candidates in the Conservative leadership election have committed to continue with the Bill, although Rishi Sunak has echoed the concerns of some other Conservative MPs around its potential impact on legal speech.

Section 2 Topic-specific snapshot: "Data access and transparency: Establishing governance structures for data access"

This section presents an overview of selected policy proposals, incoming laws and acts in DPL member countries, focusing on regulatory and non-regulatory initiatives, to outline the proposed governance structures for providing platform transparency and access for external researchers.

European Union

Data access provisions	**Digital Services Act (DSA)** **Status** Approved legislative act *Article 31 Data access and scrutiny*
Which online services	• Providers of very large online platforms which reach a number of average monthly active users in the Union equal to or higher than 45 million (Art. 25)
Which types of data	• Real-time data where technically possible, provided that the data is publicly accessible in the online interface; for example, aggregated interactions with content from public pages, public groups, or public figures, including impression and engagement data such as the number of reactions, shares, comments (r. 64).
Who should have access to data	• Digital Services Coordinator (DSC) of establishment or the Commission, upon reasoned request and within a reasonable period; • Upon a reasoned request from the DSC of establishment, vetted researchers for the sole purpose of conducting research that contributes to the detection, identification and understanding of systemic risks in the Union; • Vetted researchers should be affiliated to a research organisation (Art. 2 Directive (EU) 2019/790); independent from commercial interests; and in a capacity to preserve the specific data security and confidentiality requirements; • The application must disclose the funding and justify the necessity and proportionality of the data requested; • The researcher must commit to making their research results publicly available free of charge; • Final decision to award the status of vetted researcher lies within the competence of DSC of establishment.
How to safeguard data protection and privacy	• DSC and Commission to use data access only for the purpose of monitoring and assessing compliance; • DSC and Commission to take due account of the rights and interests of providers and users, including the protection of personal data, confidential information (trade secrets), and maintaining security of the service; • Delegated acts to lay down the specific conditions and relevant objective indicators, as well as procedures and independent advisory mechanisms in support of sharing of data with researchers; • Providers should anonymise or pseudonymise personal data except in those cases that would render impossible the research purpose pursued (r. 64).
Which mechanisms for data access	• Through appropriate interfaces specified in the request, including online databases or application programming interfaces (APIs).

European Union

Data access provisions	**2022 Strengthened Code of Practice on Disinformation** **Status** Signed voluntary code *VI. Empowering the Research Community*
Which online services	• 34 Signatories (see the list of Signatories here).
Which types of data	• Non-personal data and anonymised, aggregated or manifestly-made public data for research purposes on Disinformation (commitment 26).
Who should have access to data	• A research proposal is qualified if it is in line with relevant sector-related ethical and methodological best practices as laid down, for example, in the EDMO proposal for a Code of Conduct on Access to Platform Data; • Signatories acknowledge that the research community can include civil society organisations whose primary goal is to conduct scientific research on a not-for-profit basis, pursuant to a public interest mission recognised by a Member State; • An independent, third-party body will vet researchers and research proposals, developed by Signatories and other relevant organisations such as the European Commission (commitment 27).
How to safeguard data protection and privacy	• Signatories will describe the tools and processes in place to ensure reasonable safeguards to address risks of abuse, e.g., API policies prohibiting malicious or commercial uses (commitment 26).
Which mechanisms for data access	• Real-time or near real-time, machine-readable access through automated means such as APIs or other open and accessible technical solutions allowing the analysis of data (commitment 26).

Germany

Data access provisions	**Network Enforcement Act (NetzDG)** **Status** Legislative act entered into force) *§ 5a Information for scientific research*
Which online services	• Provider of a social network with equal to or more than two million registered users in Germany.
Which types of data	• A researcher may request qualified information about the dissemination and engagement of content which is subject to complaints or removal, including training data for the automated detection of illegal content; • Requested data must be necessary to conduct scientific research in the public interest, i.e. researching the nature, scope, causes and effects of public communication on social networks.
Who should have access to data	• Any natural or legal person who conducts scientific research; • Social networks shall be entitled to reimbursement from the researcher of reasonable costs of up to 5000 EUR.
How to safeguard data protection and privacy	• Researchers must develop a data protection concept, for example, a description of the precautions taken to prevent the information from being used for any other purposes, or a description of technical and organisational measures to ensure the protection of personal data; • Data to be transmitted anonymously or at least pseudonymously, insofar as this is possible without jeopardising the purpose of the research.
Which mechanisms for data access	• Not specified.

United States

Data access provisions	**Platform Transparency and Accountability Act (PATA)** **Status** Introduced to Congress *A section-by-section summary of the bill is available here.*
Which online services	• Any entity subject to the jurisdiction of the Federal Trade Commission (FTC) that is a website, desktop application, or mobile application; primarily serves as a medium for users to interact with content generated by other users; and has at least 25 million unique monthly users in the U.S. (Sec. 2).
Which types of data	• The National Science Foundation (NSF) to identify the data and information that the platform will be required to make available to the qualified researchers; • At a minimum, qualified data and information must be feasible for the platform to provide; be proportionate to the needs of the qualified researchers to complete the qualified research project; and not cause the platform undue burden (Sec. 4).
Who should have access to data	• Qualified researchers must be university-affiliated and submit applications to NSF for their specific research proposal' (Sec. 2); • NSF to establish a process to solicit research applications from researchers and prescribe guidelines and criteria to determine how NSF will evaluate the applications (Sec. 4).
How to safeguard data protection and privacy	• Platform Accountability and Transparency Office (PATO) within the FTC to notify the platform of research applications, and establish privacy and cybersecurity safeguards for the use of the data in question (Sec. 4); • Such safeguards may include encryption of the data or anonymizing of data to protect the privacy of individual users (Sec. 4); • Qualified researchers must submit a pre-publication version of their research to the platform and PATO for evaluation to confirm that the analysis does not expose personal information, trade secrets, or confidential commercial information (Sec. 5).
Which mechanisms for data access	• Safe harbour to prevent platforms from taking legal action against researchers who obtain information consensually and with other certain privacy protections in place (Sec. 11); • FTC may require the reporting or disclosures to be available in a form that makes it accessible and understandable to the public, or accessible for analysis by researchers, journalists, and the public, such as through an application programming interface (Sec. 12); • FTC to exercise this authority as to certain kinds of information that are already known to be of significant interest to researchers, including an ad library, information about widely disseminated content, information about content moderation decisions, and information about algorithms (Sec. 12).

United States

Data access provisions	**The Digital Services Oversight and Safety Act (DSOSA)** **Status** Introduced to Congress *A section-by-section summary can be accessed here.*
Which online services	• Hosting services which store information provided by, and at the request of, users, and which store and disseminate information to the public. Monthly active users in the U.S. equal to or more than 10 million ('covered platform') or 66 million ('large covered platform').
Which types of data	• FTC to issue rules regarding types of information that should be made available to certified researchers, for example, information related to engagement or exposure (Sec. 10 (c)); • Large covered platforms to provide a detailed ad library (Sec. 10(f)); • Large covered platforms to provide pieces of high-reach and high-engagement public content, including engagement and exposure (Sec. 10(g)).
Who should have access to data	• Office of Independent Research Facilitation at the Federal Trade Commission (FTC) to certify researchers from academia and civil society to study the impact of content moderation processes, product design decisions and algorithms on society, politics, the spread of hate, harassment and extremism, security, privacy, and physical and mental health (Sec. 10 (a)); • Requirements to be a host organisation: be an institution of higher education or a nonprofit (501(c)(3); mission includes developing a deeper understanding of the impacts of covered platforms on society; and has the organisational capacity both to follow the information security rules issued for secure researcher access and to analyse the information provided using data science and investigative and qualitative research best practices (Sec. 10 (b)).
How to safeguard data protection and privacy	• FTC to ensure that access does not infringe upon reasonable expectations of personal privacy of users, for example, requiring covered platforms to deidentify any information that is not public content; • FTC to consider under what circumstances privacy preserving techniques such as differential privacy and statistical noise should be used (Sec. 10 (c)).
Which mechanisms for data access	• FTC to issue rules relating to manner of access, for example, considering the size and sampling techniques used to create the datasets; • FTC may sponsor a Federally Funded Research and Development Center, comprised of at least 3 host organisations, to facilitate information sharing between covered platforms and certified researchers; • Safe harbour for certified researchers that create accounts solely for a research project or collect information provided for research purposes by a user, including through a browser extension or plug-in, if the certified researcher obtains informed consent (Sec. 10(c)); • Large covered platforms to host public ad library and a detailed ad library for researchers to provide insights into discriminatory ad targeting (Sec. 10(f)); • Large covered platforms to host high-reach public content stream to bring transparency to content that platforms amplify (Sec. 10(g)).

Additional proposals

United Kingdom

The Online Safety Bill (OSB) includes provisions on transparency reporting (chapter 3), obliging providers of regulated user-to-user services and of regulated search services to produce, once a year, a report about the service. OFCOM is required to produce guidance about how OFCOM will determine which information they will require transparency reports to contain. The OSB further provides provisions on research (chapter 7), requiring OFCOM to conduct research about users' experiences of regulated services, including with regard to the handling of complaints.

With regard to researchers' access to information, OFCOM will be required to produce a report (a) describing how, and to what extent, persons carrying out independent research into online safety matters are currently able to obtain information from providers of regulated services to inform their research; (b) exploring the legal and other issues which currently constrain the sharing of information for such purposes; and (c) assessing the extent to which greater access to information for such purposes might be achieved. Following the publication of the report, OFCOM may produce guidance about the matters dealt with by the report for providers of regulated services and persons carrying out independent research into online safety matters.

New Zealand

The voluntary Aotearoa Code of Practice for Online Safety and Harms, signed by Meta, Google, TikTok, Twitch, and Twitter, includes sections on transparency as well as independent research.

Signatories commit to publish and make accessible for users their safety and harms-related policies and terms of service (Measure 39) as well as information (such as via blog posts, press releases and/or media articles) on relevant policies, processes, and products that aim to reduce the spread and prevalence of harmful content online (Measure 40). Signatories also commit to publish periodic transparency reports with KPIs/metrics showing actions taken based on those policies, processes and products (Measure 41). Signatories further commit to support independent research by supporting or participating, where appropriate, in programs and initiatives undertaken by researchers, civil society and other relevant organisations (Measure 43). Signatories will support or convene at least one event per year to foster multi-stakeholder dialogue, particularly with the research community, regarding one of the key themes of online safety and harmful content (Measure 44).

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 German Federal Foreign Office for their support for this project.