



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

Section 1 Digital policy developments

EU: Digital Services Act

Type Regulatory (Legislative act)

Status Provisionally reached agreement adopted

On 16 June 2022, the European Parliament's Internal Market Committee (IMCO) endorsed the provisionally reached agreement on the Digital Services Act (DSA) with 36 votes in favour, 5 against and one abstention (the text can be found here). This comes following a back and forth between the French presidency of the Council and the Parliament, notably regarding the French proposal to add language previously dismissed by the Parliament. Therefore, France proposed to include the controversial "stay down" obligations (which would require platforms to remove not only unlawful content but also content identical to it) in recital 28. However, amid fears of delaying the vote, the French presidency removed the contested language. Furthermore, the draft agreement, in addition to voluntary crisis protocols outlined in Article 37, introduces a "crisis response mechanism" under the umbrella of risk assessments (Article 27a) that would empower the European Commission to demand additional threat assessments from very large online platforms (VLOPs) in times of crisis.

Both the DSA and Digital Markets Act are expected to be put for a final vote in Parliament in July before they are formally adopted by the Council and published in the EU Official Journal. The DSA will enter into force 20 days after publication and the provisions will start to apply fifteen months thereafter.

EU: The 2022 Code of Practice on Disinformation

Type Regulatory (Code of Practice)

Status Signed

On 16 June 2022, the strengthened Code of Practice on Disinformation was signed and presented by 34 signatories who have joined the revision process of the 2018 Code. The new Code aims to achieve the objectives of the Commission's May 2021 Guidance, by setting a broader range of commitments and measures to counter online disinformation. Signatories commit to take action in several domains, including "demonetising the dissemination of disinformation, transparency of political advertising, ensuring the integrity of services, empowering users, enhancing the cooperation with fact-checkers, and providing researchers with better access to data". While the Code comes with a strengthened monitoring framework based on quantitative and qualitative reporting elements measuring the effectiveness of its implementation, the Commission notes, "It is for the signatories to decide which commitments they sign up to and it is their responsibility to ensure the effectiveness of their commitments' implementation." The Commission further notes that it does not endorse the code, yet it considers that, as a whole, the Code fulfils previously set out expectations.

¹We 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.

EU: Report of the European Digital Media Observatory's Working Group on Platform-to-Researcher Data Access

Type Non-regulatory (Working Group consultation)

Status Published

On 31 May 2022, the Working Group on Platform-to-Researcher Data Access of the European Digital Media Observatory's (EDMO), a hub for fact-checkers, academics and other relevant stakeholders working to combat disinformation, published its [182-page report](#). The Working Group's twelve members met regularly over the last year to consider the legal, ethical, technical, and scientific possibilities for facilitating data access. The report provides draft language intended to lay the groundwork for a Code of Conduct on Platform-to-Researcher Data Access under Article 40 of the General Data Protection Regulation (GDPR), laying out careful guidance regarding the steps both researchers and platforms must take to ensure they are in compliance with the GDPR. You can find a summary by Working Group Chair Dr. Rebekah Tromble [here](#).

UK: Online Safety Bill (OSB)

Type Regulatory (Legislative act)

Status Introduced in Parliament

Line-by-line scrutiny of the Online Safety Bill by The Public Bill Committee is now underway, with four sessions a week scheduled until the end of June. During the first week's hearings, Committee members made frequent references to the complexity of the Bill. The committee sittings held on 7 and 9 June discussed various issues, including:

- The extent to which the Bill is future-proof;
- Whether cross-platform risks are dealt with sufficiently;
- Transparency requirements in regard to risk assessments (Fifth sitting, see transcript [here](#));
- Senior oversight and accountability for children's risk assessments;
- Intersectionality of harms that reflect structural inequalities in society (Sixth sitting, see transcript [here](#));
- Complaints and report handling (Seventh sitting, see transcript [here](#)); and
- Duties on fraudulent advertising on search engines (Eighth sitting, see transcript [here](#)).

France: Public consultation on access to data from online platforms for research purposes

Type Non-regulatory (Public consultation)

Status Open

On 25 May 2022, with regard to the data access provisions in the Digital Services Act (specifically Article 31), the French Regulatory Authority for Audiovisual and Digital Communication (Arcom) launched a "public consultation on access to data from online platforms for research purposes". With this consultation, Arcom intends to "to open up the debate to all participants in the digital information ecosystem and to encompass new categories of actors that could emerge in the short or medium term and fall into the "platforms" category". Arcom notes that Article 31 of the DSA, which regulates researchers' access to the data of very large online platforms in order to contribute to the assessment of the systemic risks that their services may pose, raises questions "of its full operationality". The consultation thereby considers a broader set of questions around the role of the "Digital Services Coordinator", the data covered by the new access provisions, and the status of researchers authorised to access data. The aim of the consultation is to inform the implementation of an operational framework for accessing data from online platforms. Stakeholders, including from academia, industry, government and civil society, are invited to send contributions to Arcom by 22 July.

US: American Data Privacy and Protection Act (ADPPA)

Type Regulatory (Legislative act)

Status Draft Bill introduced

On 3 June 2022, Congress [reached a major milestone](#) in the effort to produce a comprehensive data privacy framework when bipartisan members of the House Committee on Energy and Commerce and the Senate Committee on Commerce, Science, and Transportation [released a draft bill](#) for discussion—the American Data Privacy and Protection Act (ADPPA). According to the released statement, the Bill would:

- Grant American citizens broad protections against the discriminatory use of their data;
- Impose a baseline duty on all covered entities not to unnecessarily collect or use covered data in the first instance, regardless of any consent or transparency requirements;
- Prohibit any conditioning of the services by having individuals waive privacy rights;
- Require covered entities to allow consumers to turn off targeted advertisements;
- Provide enhanced data protections for children and minors;
- Provide exemptions for certain small and medium-sized covered entities.

The law would apply to all organisations, including non-profits and telecoms, and create a new division within the Federal Trade Commission (FTC) tasked with enforcement. The law would require large data holders “that use algorithms” to assess their algorithms annually and submit annual algorithmic impact assessments to the FTC, detailing steps they are taking to mitigate potential harm from their algorithms. You can find a Section by Section Summary [here](#). The Information Technology and Innovation Foundation (ITIF) [published](#) a review of the proposed Bill.

US: Establishment of the White House Task Force to Address Online Harassment and Abuse

Type Non-regulatory (Task Force)

Status Adopted

On 16 June 2022, the U.S. President established a “White House Task Force to Address Online Harassment and Abuse”, [directing](#) the Director of the White House Gender Policy Council and the Assistant to the President for National Security Affairs to lead an interagency effort to address online harassment and abuse. This Task Force focuses on technology-facilitated gender-based violence to develop concrete recommendations to improve prevention, response, and protection efforts through programmes and policies in the United States and globally. A factsheet can be found [here](#).

Section 2 Topic-specific snapshot: “In review: Government and platform responses to information manipulation regarding the invasion of Ukraine”



This section presents an overview of selected platform and government measures taken in response to Russian disinformation and war propaganda. Platform responses are considered along three categories:




1. Enforcing existing or updated Terms of Service, including content moderation policies;
2. Labelling and down ranking content;
3. Banning advertisements and de-monetising disinformation.

The snapshot of government responses focuses on measures tackling disinformation and war propaganda via broadcasting, online services (social media and search engines) and other measures such as sanctioning individuals. For a full chronology of government and companies’ measures, there are several existing trackers such as the [Technology and Social Change Project](#) at Harvard University’s Shorenstein Center and [The Tow Center](#).

Platform responses	Enforcing Terms of Service	Labelling and down-ranking content	De-monetising disinformation
Meta	<p>27 February: Meta <u>removed</u> a network of about 40 accounts, Pages and Groups on Facebook and Instagram for violating the policy against “coordinated inauthentic behaviour”.</p> <p>10 March: Meta temporarily <u>made</u> allowances for hate speech and death threats directed toward Russian and Belarusian military personnel or politicians. It later <u>said</u>, “there is no change in our hate speech policies as far as the Russian people are concerned”.</p>	<p>1 March: Meta <u>demoted and labelled</u> Facebook and Instagram posts that include links to Russian state media on Facebook and Instagram (downranking posts in Feed, and placing them lower in the Stories tray).</p>	<p>26 February: Meta <u>prohibited</u> Russian state media from running ads or monetising on its platforms.</p>
Twitter	<p>4 March: Twitter <u>banned</u> more than 100 accounts that promoted a pro-Russian hashtag, #IStandWithPutin, for “participating in coordinated inauthentic behavior”.</p> <p>10 March: Twitter <u>removed</u> tweets by the Russian Embassy in the UK for violating its “hateful conduct” and “abusive behavior” policies.</p>	<p>16 March: Twitter <u>paused</u> recommending tweets from people not followed on the Home timeline in Russia and in Ukraine.</p> <p>16 March: Twitter <u>labelled and reduced</u> the visibility of tweets that contain links to Russian state-controlled media, contributing to a 30% reduction of the reach of this content.</p>	<p>26 February: Twitter temporarily <u>paused</u> all ads in Ukraine and Russia “to ensure critical public safety information is elevated and ads don’t detract from it”.</p>

Platform responses	Enforcing Terms of Service	Labelling and down-ranking content	De-monetising disinformation
YouTube	<i>9 April:</i> YouTube <u>blocked</u> Russian parliament channel Duma TV.	<i>26 February:</i> YouTube <u>limited</u> recommendations to channels controlled by state-controlled entities.	<i>26 February:</i> YouTube <u>blocked</u> state-owned media outlets from monetizing and running ads on their channels.
Reddit		<i>1 March:</i> Reddit <u>restricted</u> access to the r/Russia and r/RussiaPolitics subreddits preventing them from showing up in searches, recommendations or feeds.	
Snapchat		<i>1 March:</i> Snapchat <u>announced</u> that its “Discover” page will only feature content from verified media partners and creators, and we have never allowed Russian state media to distribute content.	<i>1 March:</i> Snapchat stopped allowing Russian and Belarussian entities from running ads.

Government responses	Broadcasting services	Online services	Others
 Canada	<i>16 March:</i> The Canadian Radio-television and Communications Commission <u>removed</u> RT and RT France from its authorised list of non-Canadian programming services and stations.	<i>9 March:</i> The Prime Minister <u>announced</u> \$13.4 million over five years to renew and expand the <u>G7 Rapid Response Mechanism (RRM)</u> . RRM Canada also undertakes social media analysis with a particular interest in understanding the disinformation landscape.	<i>6 March:</i> Canada further <u>amended</u> the Special Economic Measures (Russia) Regulations to add 10 current or former senior government officials and their close associates, as well as agents of disinformation.
 EU	<i>2 March:</i> The Council of the EU <u>suspended</u> the broadcasting activities of Sputnik’ and RT in the EU, or directed at the EU. <i>3 June:</i> The Council of the EU <u>suspended</u> the broadcasting activities of another three Russian State outlets – Rossiya RTR/RTR Planeta, Rossiya 24/Russia 24, and TV Centre International. The advertising of products or services on sanctioned outlets has also been prohibited.	<i>4 March:</i> The European Commission sent a request to Google to remove content of RT and Sputnik from search results delivered to users located in the EU. The request notes that social media must prevent users from broadcasting any content of RT and Sputnik.	<i>8 April:</i> The Council of the EU <u>imposed</u> restrictive measures on an additional 217 individuals and 18 entities, including proponents of disinformation and information manipulation, systematically spreading the Kremlin’s false narrative on the situation in Ukraine.

Government responses	Broadcasting services	Online services	Others
 New Zealand			<p>10 May: The Foreign Ministry <u>imposed</u> new sanctions targeting eight individuals and entities involved in Putin’s campaign of disinformation, as well as cyber-attacks on Ukraine. This expands the sanctions list to include a notorious “troll farm”, the spokesperson of the Russian Ministry of Defence, and others.</p>
 UK	<p>18 March: Under the <u>Broadcasting Code</u>, Ofcom <u>revoked</u> RT’s licence to broadcast in the UK. The decision came amid 29 investigations into the due impartiality of RT’s news and current-affairs coverage of Russia’s invasion of Ukraine.</p>	<p>23 March: The Ministry of Defence <u>asked</u> YouTube to take down modified and edited clips of weaponry.</p>	<p>4 May: The Foreign Office <u>sanctioned</u> significant individuals at Channel One, a major state-owned outlet in Russia, as well as strategic propaganda organisations, including all Russia State Television and Radio Broadcasting.</p>
 US	<p>8 May: Department of the Treasury’s Office of Foreign Assets Control (OFAC) <u>banned</u> three of Russia’s state-controlled television stations.</p>		<p>3 March: Department of the Treasury’s Office of Foreign Assets Control (OFAC) <u>sanctioned</u> 26 Russia- and Ukraine-based individuals and seven Russian entities in connection with efforts to spread disinformation and influence public perceptions.</p>

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.