



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, 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

Canada: Call for proposals to tackle disinformation through Digital Citizen Initiative (DCI)

Type Non-regulatory

Status Published

On 16 March 2022, Canadian Heritage, [announced](#) the launch of a special, targeted call for proposals totalling \$2.5 million over four years to fund initiatives that help citizens identify mis- and disinformation online. Through the [Digital Citizen Contribution Program](#) and the Digital Citizen Initiative (DCI), the Government aims to increase civic literacy, promote critical thinking when it comes to validating sources of information, and build capacity in Canada to fight disinformation online. The DCI is also supporting the Public Policy Forum's [Digital Democracy Project](#), which brings together academics, civil society and policy professionals to support research and policy development on disinformation and online harms, as well as MediaSmarts' [Media Literacy Week](#).

EU: Sanctions against Kremlin-backed outlets RT and Sputnik

Type Regulation (Non-legislative acts)

Status Adopted

On 2 March 2022, the EU Member States [imposed](#) restrictive measures "in response to Russia's unprovoked and unjustified military aggression against Ukraine", suspending the broadcasting activities of Sputnik and Russia Today (RT English, RT UK, RT Germany, RT France, and RT Spanish) in the EU, or directed at the EU. The regulation [prohibits](#) operators "to broadcast or to enable, facilitate or otherwise contribute to broadcast, any content by [RT and Sputnik], including through transmission or distribution by any means such as cable, satellite, IP-TV, internet service providers, internet video-sharing platforms or applications, whether new or pre-installed". All relevant licences, authorisations and distribution arrangements are suspended. Noting the "gravity of the situation", the Council and Commission estimate such restrictive measures to be consistent with the right to freedom of expression and information as recognised in Article 11 of the Charter of Fundamental Rights. Measures will be in place "until the aggression against Ukraine is put to an end".

In the course of EU measures, Google [removed](#) RT and Sputnik from Search results. Meta [restricted](#) access to Russia's state-owned outlets. The Tow Center of Columbia University's Graduate School of Journalism [is tracking](#) actions taken globally by platforms, publishers, and governments that affect the information ecosystem in Russia and Ukraine.

On 16 March 2022, the European Parliament's Internal Market Committee (IMCO) [discussed](#) the Commission's actions as well as its cooperation with online platforms with Internal Market Commissioner Thierry Breton. Breton stressed that "propaganda of war" does not fall under the freedom of expression. In this context, Breton emphasised the important role of the upcoming Digital Services Act (DSA), including its anticipated provisions on crisis protocols.

¹ We welcome any feedback from DPL members regarding additional developments. Looking ahead, we also welcome own submissions from DPL members who wish to be featured in the digest.

EU: Digital Markets Act (DMA)

Type Regulatory (Legislative act)

Status Provisional text agreed

On 25 March 2022, the Council and the Parliament reached a provisional political agreement on the Digital Markets Act (DMA). The DMA will ban harmful business practices (such as preventing users from un-installing any pre-installed software or app) by very large online platforms that act as gatekeepers for a large number of users. For a platform to qualify as a gatekeeper, it must offer core platform services like marketplaces, app stores or search engines and have at least 45 million monthly end users and at least 10 000 business users established in the EU. Moreover, it must either have had an annual turnover of at least EUR 7.5 billion within the EU in the past three years, or have a market valuation of at least EUR 75 billion. Amazon, Apple, Google and Facebook will be among several other large companies that are affected by the DMA. Once the final legal text is approved by the Council and the Parliament, the regulation must be implemented within six months after its entry into force. A finalized text would take effect sometime in October 2022, Commissioner for Competition Margrethe Vestager said.

EU: Media Freedom Act

Type Regulatory (Legislative act)

Status Public consultation closed

On 25 March 2022, the European Commission closed a public consultation, launched on in January 2022 to collect views on issues affecting the functioning of the internal media market, including different types of interference in media. The Directorate-General for Communications Networks, Content and Technology (DG CNECT) is leading the legislative work. The Media Freedom Act is planned for adoption in the third quarter of 2022, building on the revised Audiovisual Media Services Directive, which lays down rules for the independence of media regulators. It also aims to complement the Recommendation on the protection, safety and empowerment of journalists, the proposed Digital Services Act (DSA), and the initiative to protect journalists and rights defenders from abusive litigation (SLAPP). The Act will cover:

- Transparency and independence (scrutiny of media market transactions, transparency of media ownership and audience measurement);
- Conditions for market functioning (exposure of the public to a plurality of views, media innovation);
- Air allocation of state resources (independence of public service media, distribution of state advertising);
- Governance options that could build on the European Regulators' Group for Audiovisual Media Services (ERGA).

France: Publication of the Bronner Commission report

Type Non-regulatory (Public consultation)

Status Published

On 11 January 2022, professor Gérald Bronner, who led a 14-member commission made up of academics, journalists, historians and civil society representatives, submitted the report entitled "Enlightenment in the Digital Age" to President Macron. Addressing mis- and disinformation as well as hate speech on social media, the report calls for more research on how platforms affect informational environments. The report also asks platforms to take stronger measures to prevent disinformation actors from benefiting from algorithmic promotion or advertising revenue. President Macron gave a speech warning that online platforms and foreign "propaganda" media were the main drivers behind the spread of disinformation. Macron also backed a peer review-like "self-regulation" system whereby the press industry identifies "reliable media". The fight against disinformation comes amid the finalisation of the Digital Services Act (DSA), one of France's priorities during its presidency of Council of the EU, and ahead of the presidential elections in April 2022.

US: Digital Services Oversight and Safety Act of 2022

Type Regulatory

Status Introduced into the House

On 18 February 2022, Congresswoman Lori Trahan introduced the [Digital Services Oversight and Safety Act of 2022](#) into the House. The Bill would establish a Bureau of Digital Services Oversight and Safety at the Federal Trade Commission (FTC) to conduct investigations and issue a series of evidence-based nonbinding guidance on best practices for providers of large platforms to address systemic risks (the dissemination of illegal content, individual discrimination, and any malfunctioning or intentional manipulation of a hosting service). Guidance would focus on product design features and content moderation processes that aim to be content neutral. The Bill would oblige large platforms, i.e., hosting services with 66 million monthly active users (20 % of the US population) to:

- Publish public facing community standards and transparency reports;
- Establish internal complaint handling systems to offer users the ability to appeal account and content removals;
- Make data available to certified researchers in a privacy preserving manner;
- Publish risk assessments and risk mitigation reports aimed to incentivize platforms to consider systemic risks throughout the design and operation of their products;
- Receive an independent audit of their safety practices (similar to civil rights audits);
- Provide users with insight and control into how their personal data is used in recommendation algorithms;
- Provide certified researchers (and the public as determined by the FTC) with a detailed advertisement library and high reach content stream.

UK: Online Safety Bill (OSB)

Type Regulatory

Status Introduced in Parliament

On 17 March 2022, the UK government [introduced](#) the revised Online Safety Bill (OSB) the House of Commons. This is the first step in its passage through Parliament to become law. It follows a review by a cross-party Parliamentary Joint Committee following the publication of the original draft Bill in May 2021. The bill introduces duties of care for firms hosting user-generated content, i.e., those allowing users to post their own content online or interact with each other, and for search engines. Platforms in scope will need to tackle and remove illegal material online, particularly material relating to terrorism and child sexual exploitation and abuse. The “largest, highest-risk” platforms (whose threshold will be set by the DCMS Secretary of State, in consultation with the communication regulator, Ofcom) will be required to address “legal but harmful” categories of content that will be set out in secondary legislation by Parliament. The modifications from the draft bill include:

- Bringing paid-for scam adverts on social media and search engines into scope to [combat online fraud](#);
- Including the following new [priority illegal offences](#) on the face of the primary legislation: Encouraging or assisting suicide; Offences relating to sexual images; Incitement to and threats of violence; Hate crime; Public order offences; Drug-related offences; Weapons / firearms offences; Fraud and financial crime; Money laundering; Controlling, causing or inciting prostitutes for gain; and Organised immigration offences
- Adding [harmful online communications offences](#), i.e., genuinely threatening, harms-based and false communications offences;
- Ensuring [all websites which publish or host pornography](#), including commercial sites, put robust checks in place to ensure users are 18 years old or over;
- Adding new measures to [clamp down on anonymous trolls](#) to give users more control over who can contact them and what they see online;
- Making firms proactively tackle the priority offences, i.e., ensuring features, functionalities and algorithms of their services are designed to prevent their users encountering them;
- Making firms’ senior managers criminally liable for failing to attend or providing false information in interviews with Ofcom.

Section 2 Topic-specific snapshot: “Enforcing risk assessments of online platforms”

The table below presents selected provisions regarding governance structures, implementation and enforcement of risk assessments and audits, including recently proposed regulatory and self-regulatory approaches.

EU: Digital Services Act (DSA)

Governance Structures / Regulator(s)

Digital Services Coordinators (DSCs): National authorities designated by each Member State responsible for the application and enforcement (Art. 38, Art. 39). Where the DSC of destination (i.e., where the service is provided) has reason to suspect that a provider infringed obligations under the regulation, it shall request the DSC of establishment (i.e., where the provider is established/its legal representative resides) to assess the matter and take the necessary measures to ensure compliance.

- Where the DSC of destination (i.e., where the service is provided) has reason to suspect that a provider infringed obligations under the regulation, it shall request the DSC of establishment (i.e., where the provider is established/its legal representative resides) to assess the matter and take the necessary measures to ensure compliance.

European Board for Digital Services: Independent advisory group for the Commission, composed of DSCs and, where appropriate, other competent authorities; coordinates joint investigations; issues opinions and recommendations (Art. 47, Art. 48, Art. 49).

European Commission: In case of enforcement related to systemic risks of VLOPs, the Commission may intervene via binding decisions (‘enhanced supervision’) (Art. 50).

Compliance Structures

Very Large Online Platforms (VLOPs) are obliged to carry out risk assessments in relation to the functioning and use of their services. VLOPs must identify systemic risks related to the dissemination of illegal content, any negative effects for the exercise of certain fundamental rights, and the intentional manipulation of their service (Art. 26).

VLOPs shall be subject, at their own expense and at least once a year, to audits to assess compliance (Art. 28).

The audit report should help inform and, where appropriate, suggest improvements to the measures taken by the VLOPs. It should be transmitted to the DSC of establishment and the Board without delay, together with the risk assessment and the mitigation measures, as well as the platform’s plans for addressing the audit’s recommendations (r.61).

Audits shall be performed by organisations which:

- Are independent from the VLOP concerned;
- Have proven expertise in the area of risk management, technical competence and capabilities;
- Have proven objectivity and professional ethics, based in particular on adherence to codes of practice or appropriate standards (Art. 28).

VLOPs shall appoint compliance officers who should:

- Cooperate with the DSCs of establishment and the Commission;
- Organise and supervise the VLOPs activities relating to the audit (Art. 32).

Enforcement Structures

DSC investigative powers:

- Requesting platforms as well as any other persons that may reasonably be aware of information relating to a suspected infringement to provide information;
- Conducting on-site inspections of any premises of platforms;
- Interviewing any member of staff of providers to give explanations in respect of any information;

Enforcement Structures
(continued)

DSC enforcement powers:

- Making the platforms' commitments binding;
- Ordering cessation of infringements;
- Imposing fines and periodic penalty payments;
- Where the infringement persists and causes serious harm: Requiring providers to examine the situation, adopt and submit an action plan setting out the necessary measures to terminate the infringement (Art. 41);
- Participate in joint investigations, which may be coordinated with the support of the Board, concerning providers operating in several Member States (Art. 46).

Where the DSC finds that a VLOP has infringed the systemic risks obligations, it shall make use of the enhanced supervision. Acting on its own initiative, the Commission*:

- May recommend the DSC of establishment to investigate the suspected infringement;
- Can carry out investigations, including through requests for information (Art. 52), interviews (Art. 53) and on-site inspections (Art. 54);
- Can adopt interim measures (Art. 55) and make binding commitments (Art. 56);
- Adopt non-compliance decisions (Art. 58), as well as fines not exceeding 6% of it's the VLOPs total turnover (Art. 59) and periodic penalty payments for breaches, as well as for supply of incorrect, incomplete or misleading information (Art. 60).

*The agreed [Council general approach](#):

- Grants the Commission exclusive powers for supervision of VLOPs;
- Requires the Commission and the DSCs to provide each other mutual assistance, particularly as regards exchange of information.

 Ireland: [Online Safety and Media Regulation Bill 2022](#)

Governance Structures / Regulator(s)

Establishment of a new regulator, the Media Commission; and dissolution of the existing regulator, the Broadcasting Authority of Ireland.

Compliance Structures

The Media Commission may appoint an independent person to carry out an audit of a designated online service's complaints and complaints-handling process in order for the Commission to assess compliance with an online safety code, and provide the Commission with information to identify trends in complaints or other matters.

Enforcement Structures

The Media Commission has the power:

- To impose industry levies to fund its operations;
- To require the provision of information from regulated services;
- To seek appointment of authorised officers to investigate contraventions;
- To seek to impose administrative financial sanctions of up to €20 million or 10% of turnover in respect of non-compliance;
- To issue notices to end non-compliance;
- To seek the prosecution of senior management of designated online services for failure to comply with a notice to end non-compliance;
- To seek to block access to certain online services; and
- To issue content limitation notices to designated online services in respect of individual pieces of harmful online content.

 **Netsafe - New Zealand’s independent online safety organisation:
Code of Practice for Online Safety and Harms**

**Governance
Structures /
Regulator(s)**

Administrator: Organisation agreed upon and appointed by the Signatories to oversee the administration of the Code.

Sub-committee: Comprised of representatives from the Signatories, Maori cultural partners, civil society and other relevant and agreed-upon stakeholders.

**Compliance
Structures**

A complaints mechanism:

- Will enable the public to report breaches by Signatories of their Code commitment;
- Will establish the criteria for determining non-compliance and appropriate redress mechanism(s) for Signatories to respond to complaints.

Compliance mechanisms:

- An annual compliance report will be provided by Signatories, setting out the measures implemented.
- The administrator will publish and make publicly available an analysis of Signatories’ reports and their progress.
- The sub-committee will meet annually to review how Signatories are meeting their commitments, including assessing Signatories’ annual compliance reports; complaints submitted through the Complaints Mechanism; and progress of the Code.

Administrator’s powers are :

- To make any public comments about the Code and may name individual Signatories for positive or negative progress, where there is a proper basis to do so (the Administrator must provide reasonable notice and consult with the Signatory before making public comments about the Signatory with respect to the Code);
- To recommend to the Sub-committee the termination of a signatory, based on repeated failures to comply with the commitments of the Code;
- To initiate the termination process of a signatory for repeated non-compliance and issue a public announcement (after consultation with the Sub-committee).

 **UK: Draft Online Safety Bill (OSB)**

**Governance
Structures /
Regulator(s)**

Ofcom, the communications regulator, will be appointed as the regulator for the Online Safety regime.

Ofcom’s duties will be:

- To carry out impact assessments;
- To assess each regulated user-to-user service and establish a register of particular categories of services;
- To carry out risk assessments to identify and assess risks of harm and publish register of risks and risk profiles;
- Produce guidance to assist services in complying with their duties to carry out illegal content risk assessments;
- Publish codes of practice, setting out the steps a company should take to comply with their new duties.

Compliance Structures

“Category 1 services” will have a duty to carry out a suitable and sufficient adults’ risk assessment (including, e.g., level of risk of functionalities of the service).

Ofcom’s powers include:

- Powers to require information (‘information notices’);
- Skilled persons’ reports (i.e., appoint a skilled person to provide Ofcom with a report about identifying and assessing a failure);
- Investigations (into whether a provider of a regulated service is failing to comply with any requirement);
- Powers to require interviews;
- Powers of entry, inspection and audit (Schedule 11);
- Information offences and penalties, including senior managers’ liability (bring criminal sanctions against senior managers who fail to ensure their company complies with information requests);
- Co-operation and disclosure of information: overseas regulators.

Enforcement Structures

Ofcom’s enforcement powers include:

- Provisional notice of contravention (will set out steps the provider must take to comply, or impose a penalty of up to £18 million or 10 % of qualifying worldwide revenue);
- Confirmation decisions (including imposing a requirement to take steps to use proactive technology to identify illegal content and ensure children are not encountering harmful material).

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.