

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: eSafety Commissioner review multiple Online Safety Codes

Type Regulatory

Status Under review

On 20 May 2025, the final drafts of eight Online Safety Codes, covering a range of online services, were submitted to the online safety commissioner, eSafety, for review under the Online Safety Act. Developed by Australian industry associations, the Codes respond to concerns raised by eSafety regarding multiple drafts submitted since October 2024. Each Code sets out service-specific compliance obligations based on risk tier, aimed at reducing Australians' exposure to Class 1C and Class 2 material, including high-impact pornography, self-harm content and violent material. Mandatory measures include age assurance, access controls, content moderation, user reporting mechanisms and transparency requirements. Providers are required to undertake risk assessments, engage with eSafety and submit compliance reports upon request. Where a Code is deemed inadequate, eSafety may determine an enforceable industry standard in its place.

European Union: European Commission concludes consultation on enhanced online privacy and safety guidelines for minors

Type Regulatory (consultation)

Status Closed

On 10 June 2025, the European Commission closed its consultation on guidelines aimed at enhancing online protection for minors under the Digital Services Act (DSA). These guidelines focus on online privacy, safety, and security for child-accessible platforms, proposing measures like age assurance mechanisms to limit children's exposure to inappropriate content, default private settings for children's accounts, and adjusted recommender systems prioritising user feedback. Recommendations also suggest children to block and mute users and require explicit consent for group participation to mitigate cyberbullying risks. The final guidelines are expected by the end of Q3 2025.

European Union: European Commission investigates Pornhub, XNXX, XVideos and Stripchat over suspected DSA breaches related to the protection of minors

Type Regulatory (investigation)

Status Ongoing

On 27 May 2025, the European Commission announced formal proceedings under the DSA against the adult platforms Pornhub, XNXX, XVideos, and Stripchat for suspected failures to protect minors, citing insufficient age verification, risk assessments, and safeguards. While Pornhub, XNXX and XVideos remain designated Very Large Online Platforms (VLOPs)

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.

under direct Commission supervision, the press release announced Stripchat's de-designation as a VLOP, with its VLOP obligations ending in four months. Stripchat will continue to be subject to general DSA duties and supervised by Cyprus's Digital Services Coordinator (DSC). However, [legal action](#) against Cyprus for failing to empower its DSC raises concerns about effective oversight. The Commission will conduct detailed investigations and may take further measures.

European Union: European Parliament committee endorses tougher measures against child sexual abuse and exploitation

Type Legislative (proposal)

Status Pending parliamentary debate

On 13 May 2025, the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) [adopted](#) its position on a [revised draft Directive on combating the sexual abuse and sexual exploitation of children and child sexual abuse material](#). The draft proposes increasing maximum sentences for child sexual abuse offences and eliminating time limits for prosecution. It also criminalises the use of AI for such offences, endorses measures against the online distribution and livestreaming of abuse, and allows third-party organisations to report these crimes. The European Parliament will debate and vote on this position from 16 to 19 June 2025.

Canada: Consultation on age verification requirements in Children's Privacy Code under the Personal Information Protection and Electronic Documents Act

Type Regulatory (consultation)

Status Open

On 12 May 2025, the Office of the Privacy Commissioner of Canada (OPC) [launched](#) a consultation on the development of a [Children's Privacy Code](#) under the [Personal Information Protection and Electronic Documents Act \(PIPEDA\)](#). The consultation focuses on data protection regulation relating to collecting, using, disclosing, retaining, and safeguarding children's personal information. The proposed Code aims to clarify organisational responsibilities concerning meaningful consent, data minimisation, privacy by default, and limitations on certain data practices, particularly online. The consultation is open until 5 August 2025.

Ireland: Data Protection Commission issues statement on Meta's use of users' data for AI training

Type Regulatory (monitoring)

Status Ongoing

On 21 May 2025, the Data Protection Commission (An Coimisinéir Cosanta Sonraí) (DPC) [issued](#) a statement on Meta AI's handling of personal data for training Large Language Models (LLMs) in the EU/EEA. Following discussions that began in March 2024, the DPC raised concerns about Meta's planned use of publicly available content from Facebook and Instagram, leading to a temporary suspension in June 2024. The DPC also sought an [Opinion](#) from the European Data Protection Board (EDPB), which outlined criteria for assessing General Data Protection Regulation (GDPR) compliance in AI model training. In response, Meta revised its approach, introducing enhanced safeguards, including updated transparency notices, improved mechanisms for objections, longer user notification periods, and technical measures like data de-identification and output filtering. The DPC continues to monitor compliance, requiring Meta to submit an evaluation report by October 2025. Users are advised to check their privacy settings to manage data usage.

New Zealand: Deepfake Digital Harm and Exploitation Bill introduced in Parliament

Type Legislative (Member's Bill)

Status Introduced

On 12 May 2025, the Deepfake Digital Harm and Exploitation Bill was introduced to the New Zealand Parliament. The Bill seeks to amend both the Crimes Act 1961 and the Harmful Digital Communications Act 2015 by expanding the definition of an intimate visual recording to include digitally altered or synthesised images. Its purpose is to tackle the growing issue of sexually explicit deepfakes and to strengthen legal protections for individuals whose likeness is used without their consent. Under the proposed changes, intimate visual recordings would include visual content that has been created, manipulated, or synthesised to portray a person in a state of undress or engaged in intimate acts, ensuring such material falls within the scope of the relevant legal provisions and offences outlined in the revised legislation.

United Kingdom: Ofcom closes consultation on draft guidance on women and girls' online safety

Type Regulatory (consultation)

Status Closed

On 23 May 2025, Ofcom concluded its consultation on draft guidance aimed at improving online safety for women and girls. The guidance addressed issues like online misogyny, coordinated harassment, online domestic abuse, and the non-consensual sharing of intimate images, including AI-generated content and cyberflashing. It proposed practical measures such as "abusability" testing, technology to prevent image-based abuse, user prompts, enhanced account controls, and training for content moderation teams. These steps were designed to align with the UK's Online Safety Act (OSA), which mandates platforms to protect users from illegal content and safeguard children from harmful material. Final guidance is expected later this year, with an assessment of industry compliance anticipated about 18 months post-implementation.

United Kingdom: Ofcom issues guidance on tackling violent content related to knife crime

Type Regulatory (guidance)

Status Published

On 20 May 2025, Ofcom issued guidance under the OSA concerning violent content and illegal weapon sales, particularly regarding knife crime and risks to young people. The guidance expresses Ofcom's concerns about online platforms promoting violence and facilitating access to illegal weapons, which poses significant risks by normalising knife use. Online services, including e-commerce, user-to-user platforms, and search engines, must take active steps to protect UK users from content related to unlawful knife sales and violence. They are also required to implement measures to prevent children from encountering such harmful material. This guidance builds on Ofcom's previous Illegal Harms Statement and Protection of Children Codes, outlining how platforms must manage risks associated with violent and illegal content. Non-compliant providers may be face mandated changes, fines, or access restrictions.

United States: House approves budget Bill to suspend state AI laws and modernise federal IT infrastructure

Type Legislative proposal (federal)

Status Passed by the House of Representatives; pending Senate consideration

On 22 May 2025, the House of Representatives approved the Budget Reconciliation Bill, which includes the Artificial Intelligence and Information Technology Modernization initiative. The Bill imposes a ten-year federal suspension on the

enforcement of state and local laws regulating such technologies. Exceptions apply to laws that support AI deployment, simplify administrative processes, or enforce impartial, cost-based requirements similar to those applied to non-AI systems. Additionally, the Bill allocates funds to the Department of Commerce to modernise federal IT infrastructure by utilising commercial AI and automation tools to enhance efficiency, replace outdated systems, and strengthen cybersecurity. The Bill now proceeds to the Senate for consideration.

United States: Federal Trade Commission closes inquiry into technology platforms and censorship

Type Regulatory (consultation)

Status Closed

On 21 May 2025, the Federal Trade Commission (FTC) closed a public consultation concerning censorship practices by technology companies. The consultation aimed to ascertain whether platforms had breached the law by limiting users' access based on their speech or affiliations. The investigation applied to technology platforms, including social media firms, and concentrated on how their actions, including bans, shadow banning, or demonetisation, might have adversely affected consumers and competition.

United States: President signs TAKE IT DOWN ACT to criminalise non-consensual intimate imagery

Type Legislative

Status Enacted

On 19 May 2025, President Trump signed the bipartisan TAKE IT DOWN Act into law. Following the approval by the U.S. House of Representatives on 14 May 2025, with a vote of 409–2, and unanimous consent in the Senate earlier in February, the legislation is now officially enacted. The TAKE IT DOWN Act criminalises the distribution of non-consensual intimate imagery (NCII), including deepfakes. It also mandates that social media platforms and similar online services remove such content within 48 hours of receiving notice from a victim, with enforcement responsibility assigned to the Federal Trade Commission (FTC).

United States: Kids Online Safety Act reintroduced in Senate

Type Legislation (proposed)

Status Reintroduced

On 14 May 2025, the Kids Online Safety Act (SB 1748) was reintroduced in the United States Senate. The Bill seeks to establish a duty of care for online platforms in addressing potential risks to children and young people, including concerns related to mental health, compulsive usage, online abuse, and exposure to harmful content. It sets out provisions such as giving minors the ability to manage communications, restrict access to their personal data, modify design features linked to compulsive behaviour, and control personalised recommendation systems. The Bill also requires parental oversight of privacy settings, purchases, and screen time. Further provisions include mechanisms for reporting, transparency requirements, and restrictions on advertising unlawful products to minors. Additionally, it calls for research into age verification techniques and guidance on the implementation of safety measures.

Section 2 Topic-specific snapshot: “Online Hate Targeting LGBTQ+ Communities: Trends, Harms, and Responses”

This section summarises selected analyses and responses published by government agencies, civil society organisations and academia on online hate targeting LGBTQ+ communities.

Offline events, online threats: Analyzing online extremist targeting of LGBTQ+ communities,

Institute for Strategic Dialogue, 5 June 2025

Between August 2024 and January 2025, online anti-LGBTQ+ activity in the United States surged in response to real-world events, according to an analysis of over 97,000 posts across more than 1,000 accounts and channels linked to violent extremist ideologies. The findings point to a clear correlation between offline developments and spikes in online hate, with some events causing the volume of extremist activity to double. Notably, posts that included explicit “support for violence” made up 5% of the total dataset.

Transgender individuals were disproportionately targeted, particularly in the aftermath of the 2024 US elections. Transphobic content grew from 35% of all anti-LGBTQ+ material in October–November to 46% in December–January. Key flashpoints included the Transgender Day of Remembrance, misinformation about Olympic boxer Imane Khelif’s gender identity, and the signing of an executive order on “gender ideology” in January.

The analysis also found that violent extremists were primarily driven by false narratives about “grooming” and “pedophilia”, with the highest levels of engagement taking place on X (formerly Twitter) and Telegram. While racially motivated extremists initially led this activity, they were later overtaken by a mix of misogynist and conspiratorial groups, illustrating the cross-cutting nature of violent hate online. The findings underscore the importance of tracking how offline political and cultural developments can intensify digital threats against LGBTQ+ communities.

2025 Social Media Safety Index,

GLAAD, 2025

GLAAD’s 2025 Social Media Safety Index (SMSI) report, including its annual Platform Scorecard, assesses the safety, privacy, and freedom of expression for LGBTQ users across six major social media platforms: TikTok, X, YouTube, and Meta’s Instagram, Facebook, and Threads. Using 14 LGBTQ-specific indicators, the Scorecard evaluates policies and product features based on a research methodology adapted from Ranking Digital Rights. While some platforms have made improvements, others – most notably Meta and YouTube – have significantly rolled back protections, particularly for transgender and non-binary individuals.

Despite these mixed results, overall scores remain alarmingly low. This year’s Scorecard is not directly comparable to previous years due to substantial changes in the evaluation methodology, which now includes new indicators addressing

emerging threats to LGBTQ safety and expression. Key best practices against which platforms are measured include prohibiting targeted harassment such as misgendering and deadnaming, banning “conversion therapy” content, and protecting LGBTQ users from hate speech. Transparency and user privacy also remain vital, with platforms encouraged to offer pronoun options, control over data use, and regular disclosure of moderation actions.

GLAAD’s research highlights serious concerns beyond the mere existence of policies, including poor enforcement, widespread suppression of legitimate LGBTQ content, and over-moderation that unjustly targets LGBTQ creators. Transparency is limited regarding content moderation, algorithmic processes, and data privacy, while the reliance on AI moderation without adequate human oversight exacerbates these harms. These challenges disproportionately affect LGBTQ users who belong to other marginalised groups, emphasising the need for more inclusive and accountable platform practices worldwide.

The report concludes with urgent recommendations for platforms: to strengthen and restore protective policies, improve moderator training with a focus on LGBTQ issues, increase transparency through independent research collaboration, respect user privacy by reducing data collection and targeted advertising, and foster civil discourse. GLAAD stresses the importance of these actions to ensure social media remains a safe and supportive space for LGBTQ communities globally, while cautioning against legislative approaches that might inadvertently harm LGBTQ users.

A Year of Hate: Understanding Threats and Harassment Targeting Drag Shows and the LGBTQ+ Community,

Tim Squirrelrell and Jacob Davey, Institute for Strategic Dialogue, 2023

This ISD report finds that rising hate and extremism present a significant threat to human rights and democratic freedoms, with LGBTQ+ communities frequently targeted. It examines recent trends in anti-LGBTQ+ hate and focuses on the harassment at all-ages drag shows. The hate against drag events highlights key actors and tactics within anti-LGBTQ+ activism.

The report’s analysis draws on 274 anti-drag mobilisations across the US, UK, Australia, and France, alongside instances from other European countries, supported by extensive monitoring of social media platforms and external data sources.

It finds notable consistency in anti-LGBTQ+ activism globally, especially regarding tactics employed, with some geographical differences. Across all regions studied, mobilisation against drag events has united loose coalitions comprising extremists, conspiracy theorists, local activists, and fringe political figures. Far-right groups, fundamentalist religious activists, and anti-LGBTQ+ influencers on the political right are the principal drivers of this activism. Political support for anti-drag actions exists in France, Australia, and the US. However, only in the US have a substantial number of mainstream elected representatives engaged openly in anti-drag rhetoric and activities.

These groups draw on a shared narrative framework, often rooted in “save the children” conspiracy theories popularised by movements such as QAnon since 2017. This narrative is used to vilify LGBTQ+ individuals and to legitimise extreme actions purportedly necessary to protect children.

The US stands out with the highest number of protests and violent incidents related to anti-drag activism, including tragic attacks like the Club Q shooting and an attempted arson. It has also pioneered legislative measures banning drag performances, which is not the case in the other analysed countries. Additionally, US anti-drag protests often feature private planning and coalition-building across ideological lines, with public mobilisation supported by high-profile online influencers.

Globally, anti-LGBTQ+ actors employ common tactics, including doxxing, threats of violence, coordinated harassment of venues and performers, and distribution of stickers and flyers. Despite frequent threats, only a small fraction of drag performances are cancelled, with US data showing cancellations affecting just 6.4% of targeted events. Offline mobilisation tends to be highly localised, usually organised in response to specific planned events and accompanied by online coordination.

The report emphasises the urgent need to understand these hate movements in order to aid policymakers and law enforcement in effectively combating discrimination.

LGBTIQ equality at crossroads: progress and challenges,

European Union Agency for Fundamental Rights (FRA), 2024

FRA's survey is one of the largest of its kind globally, capturing the experiences of over 100,000 LGBTIQ people aged 15 and above across the EU and neighbouring countries. Now in its third wave – following previous editions in 2012 and 2019 – the survey provides a valuable picture of progress and persistent challenges over time. Its findings are intended to guide legal and policy responses that uphold the fundamental rights of LGBTIQ people. With growing concerns about safety and equality, the report emphasises that this is a critical moment for the EU and its Member States to strengthen their efforts to ensure dignity and inclusion for all.

Although many survey participants express feeling safer expressing their identity and see improved inclusion in schools, hate speech, bullying and online disinformation campaigns about LGBTQ people persist. A concerning number of LGBTIQ people expressed having suicidal thoughts, particularly trans women and trans men. Additionally, trans and intersex people, LGBTIQ people with disabilities, or those belonging to minority groups, or those who are unemployed, face increased adversity.

In view of these findings, FRA urges the EU and Member States to decisively protect LGBTIQ rights, ensure safety, and uphold dignity.

Key findings of the report include:

- **Discrimination:** Slight overall decrease (36% in 2023 vs. 42% in 2019), but trans and intersex people still face the highest rates – especially in employment and housing. Only 11% report incidents, mainly due to distrust or fear of inaction.
- **Violence and Harassment:** Hate-motivated violence rose to 14%, with intersex and trans individuals most affected. Harassment affects over half (55%) of respondents, yet 82% of violent incidents go unreported.

- **Online Hate and Mental Health:** 63% regularly encounter hateful content online. Trans, non-binary, and intersex people report higher rates of suicidal thoughts and homelessness.
- **Policy and Trust:** Trust in governments to combat anti-LGBTIQ+ bias is falling. The FRA calls for stronger legal protections, including bans on conversion practices and adoption of the Equal Treatment Directive.
- **Visibility and Safety:** More LGBTIQ people are open about their identity (52%), but 1 in 3 still avoid certain places due to fear. Public displays of affection remain a concern for many.
- **Education:** Bullying in schools increased sharply (67% in 2023 vs. 46% in 2019), with limited positive representation of LGBTIQ topics in curricula.

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.