Digital Cooperation Organization

DCO Policy Watch

Navigating the digital policy landscape

Edition 4 | April 2025

Table of contents

1 Overview

Welcome to the fourth edition of the DCO Policy Watch, a quarterly publication designed to keep policymakers, experts, and decisionmakers in DCO Member States, Observers, and stakeholders apprised of the evolving landscape in digital policy. This publication serves as a platform for sharing insightful analyses and updates on the latest trends and developments within key areas of digital governance. Our aim is to facilitate a deeper understanding of various international practices and strategies, thereby supporting our readers in informed decision making and effective policy formulation.

Since its launch in 2024, the DCO Policy Watch has explored a wide range of critical issues. The first edition examined the evolving landscape of digital policy, highlighting key trends and recent developments in **AI, Data Protection and Privacy, Electronic Waste (E-waste)**, and the **Future of Work.** The second edition focused on the evolving ecosystem of **Digital Public Infrastructure (DPI)**, with particular emphasis on the role of **Digital Government, Digital Identity**, and **Open Data** in empowering citizens through efficient service delivery, as well as setting the foundation for the future of government. The third edition explored global policy efforts particularly within DCO Member States – to **build sustainable societies, economies, and communities**, with an emphasis on policies relating to **Climate Action, EdTech, and Space Exploration** as key drivers of sustainable development.

These policy areas have continued to evolve. At the World Economic Forum (WEF) Annual Meeting in January 2025, held under the theme of *"Collaboration for the Intelligent Age"* discussions centered on inclusive growth, biodiversity conservation, and the responsible deployment of technology and AI. UN Secretary-General António

Guterres stressed the need to rebuild trust, strengthen collaboration, and bridge the digital divide, while also calling for sustainability-driven business practices and ethical AI governance. Additionally, France hosted the AI Action Summit from February 10-11, 2025, where parties, with the notable exclusion of the U.S. and the U.K., signed the "Statement on Inclusive and Sustainable AI for People and the Planet."

Building on these global discussions, the fourth edition of the DCO Policy Watch will focus on the **Responsible Digital Ecosystem and the Role of Platform Governance**. This edition examines how platform governance contributes to a responsible digital ecosystem and highlights policy efforts from both public and private sector stakeholders in fostering responsible digital platforms. It begins with a holistic analysis of the digital ecosystem before exploring the critical role of platform governance in maintaining a secure and trustworthy digital environment. The edition then delves into three key areas of platform governance—**Online Safety and Digital Trust, Content Governance**, and **Fair Competition**—outlining their significance in shaping a responsible digital ecosystem.

info@dco.org

2 Responsible Digital Ecosystem and the Role of Platform Governance

2.1 Overview

The digital age has ushered in a transformative era where digital ecosystems have become the backbone of the global economy, reshaping how individuals, businesses, and governments interact. This digital ecosystem, comprising interconnected technologies, digital platforms, and various stakeholders, drives innovation, efficiency, and inclusion. However, its rapid growth has also introduced challenges such as data privacy concerns, misinformation, and monopolistic practices. This chapter examines digital ecosystems, the need to foster their responsible development, and the crucial role of digital platform governance in ensuring their sustainability, trustworthiness, and inclusivity.

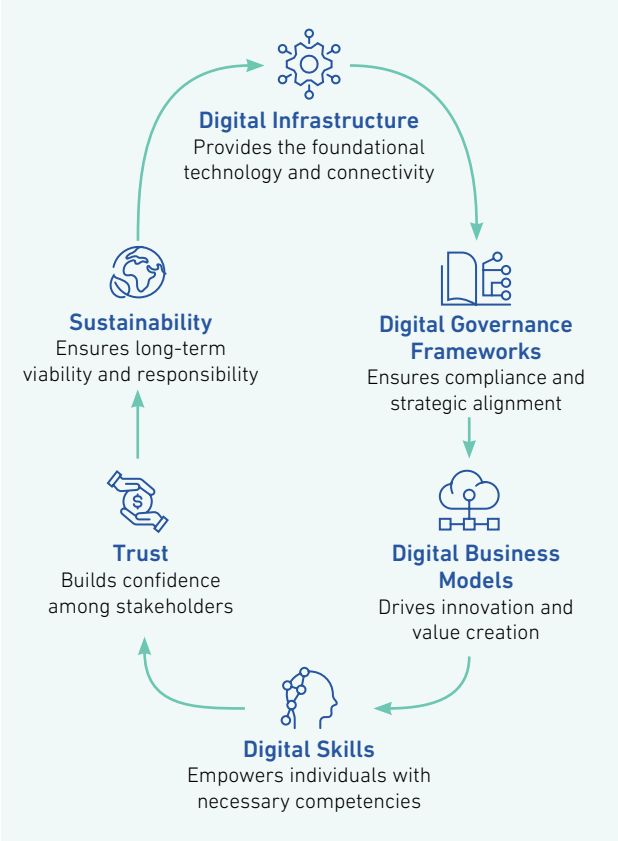
2.2 Digital Ecosystems

Digital ecosystems are complex networks of interconnected entities—comprising individuals, organizations, technologies, and processes—that interact within a digital environment to create, exchange, and consume value. These ecosystems are defined by their ability to enable collaboration, innovation, and scalability across sectors. Various definitions highlight their multifaceted nature:

- International Institute for Management Development (IMD): A digital ecosystem is a network of interconnected stakeholders, including individuals, businesses, and systems, that use digital technologies to interact, collaborate, and create value.
- International Journal of Research and Analytical Reviews (IJRAR): Digital ecosystems are complex, interdependent systems with underlying infrastructures through which all constituents interact and exhibit self-organizing, scalable, and sustainable behaviors.

From these definitions, we can identify the key components of a digital ecosystem:

Fig. 1: Components of a Digital Ecosystem



Illustrative Example of a Digital Ecosystem

Consider a smart city ecosystem where digital platforms like ride-sharing apps, e-government portals, and IoT-enabled infrastructure (e.g., smart traffic lights) interact with stakeholders such as citizens, businesses, and government agencies. This ecosystem relies on digital infrastructure (e.g., broadband networks), governance frameworks (e.g., market access/ data privacy regulations), and digital skills (e.g., coding, data analysis) to function effectively.

2.3 The Role of Digital Platforms within Digital Ecosystems

Digital platforms serve as key enablers within digital ecosystems, facilitating interactions between users, service providers, and other stakeholders. They drive innovation and economic growth across industries such as e-commerce, social networking, finance, and transportation.

Key Stakeholders in Digital Platforms

Users:
Engage with platforms for services and information, contributing to accountability through feedback and advocacy.

Governments:
Establish that balance innovation with accountability, ensuring platforms align with the public interest.

Digital Platforms/Technology Providers:
Develop and maintain platforms, setting policies on data protection, content moderation, and algorithmic governance.

Understanding the role of digital platforms within the digital ecosystem is crucial for building a responsible digital ecosystem that prioritizes ethical considerations, sustainability, and inclusivity. The following sections delve into the key dimensions of a responsible digital ecosystem.

2.4 Understanding the Responsible Digital Ecosystem

A **Responsible Digital Ecosystem** goes beyond technological interconnectivity. It prioritizes ethical considerations, environmental sustainability, and social inclusivity, ensuring that the benefits of digitalization are equitably distributed while minimizing harms such as data breaches, harmful content, misinformation, and environmental degradation. Such ecosystems are built on three key dimensions:

1. Ethical Governance

Ethical governance is the cornerstone of a responsible digital ecosystem. In this framework, platform governance ensures that digital platforms and services are developed and operated in a manner that prioritizes transparency, data protection, user safety, and ethical technology implementation.

- **Transparency:** Within a responsible digital ecosystem, effective platform governance aims to ensure that digital platforms, to the extent possible, are transparent about their algorithms, data usage, and decision-making processes, and users have clear information about how their data is collected, used, and shared.

- **Data Protection and User Safety:** Data protection and user safety refer to the safeguards that platforms incorporate to prevent misuse of user data and mitigate online harms. These include technical measures like encryption and secure authentication, compliance with data protection regulations such as the GDPR, and AI-powered content moderation. For a more detailed overview of global developments in data privacy and protection frameworks, including approaches across the European Union (EU), the Middle East and North Africa (MENA), and Asia-Pacific (APAC), see the first edition of the DCO Policy Watch, which comprehensively examined these issues.

- **Ethical Technology Implementation:** This attribute refers to the design and deployment of technology in ways that respect human rights and ethical principles. This includes avoiding algorithmic biases, ensuring fairness in AI systems, and preventing the misuse of technology for harmful purposes.

2. Economic, Environmental, and Social Sustainability

A responsible digital ecosystem also means ensuring sustainability across multiple dimensions—economic, environmental, and social. Here again, digital platforms play a crucial role in promoting sustainability through responsible business practices, equitable access, and ethical data management – such as minimizing unnecessary data collection and promoting energy-efficient data storage:

- **Economic Sustainability:** Promote fair digital markets, affordable services, and digital entrepreneurship.
- **Social Sustainability:** Ensure equitable access and digital inclusion for marginalized communities.
- **Environmental Sustainability:** Minimize ecological footprints through energy-efficient technologies and sustainable practices.

3. Digital Inclusion

Digital inclusion is essential for ensuring that the benefits of digitalization are equitably distributed. A responsible digital ecosystem is inclusive by design. Ensuring inclusion involves coordinated action by multiple stakeholders – policymakers, connectivity providers, and digital platforms – who work together to close access gaps and expand participation in the digital economy.

- **Bridging the Digital Divide:** This involves extending affordable internet access and digital devices to underserved and remote areas.
- **Ensuring Equitable Access:** Policies and technologies are designed to ensure that all individuals, including those with disabilities, can access and benefit from digital services.
- **Promoting Digital Literacy:** Educational programs enhance digital literacy and skills, enabling individuals to participate fully in the digital economy.

2.5 Policy Efforts towards Governing Digital Platforms

To ensure a responsible digital ecosystem, policymakers and regulators globally are making efforts to address key concerns and ensure responsible platform governance within the broader digital ecosystem. These areas are interconnected and contribute collectively to ensuring that platforms operate in a safe, fair, and accountable manner. These include:

- **Consumer Protection:** Safeguarding users from deceptive practices, misleading advertisements, and ensuring fair treatment by digital service providers.
- **Content Moderation:** Managing harmful or illegal content, ensuring media plurality, and addressing issues such as misinformation and hate speech.
- **Data Privacy and Security:** Implementing robust data protection measures, ensuring transparency in data collection practices, and establishing user consent mechanisms to prevent misuse of personal information.
- **Competition:** Ensuring fair market practices and preventing monopolistic behavior through regulations such as the Digital Markets Act (DMA) and Australia's Media Bargaining Code by the Australian Competition and Consumer Commission (ACCC).

While sharing similar objectives, global regulatory approaches to digital platforms vary, aiming to balance responsible governance with the need to foster innovation:

1. Consumer Protection

In the U.S., the Federal Trade Commission (FTC) plays a key role in regulating large online platforms, particularly on issues of consumer protection, data privacy, and anti-competitive conduct.

In the Asia-Pacific region, Australia's ACCC has been active in enhancing consumer protection by regulating digital platforms. India's Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 require the establishment of grievance redressal mechanisms, the appointment of compliance officers, and the implementation content of takedown procedures, ensuring greater accountability in digital services, while Singapore's Online Safety (Miscellaneous Amendments) Act of 2022 protects users, especially children, from harmful online content and ensures accountability through annual safety reports.

Across DCO Member States, consumer protection policies increasingly extend to digital platforms, including measures to enhance financial transparency. By promoting clear and fair terms for digital services and safeguarding users against fraud and deceptive practices, these initiatives strengthen trust in e-commerce and digital finance ecosystems. For example, Oman' Consumer Protection Law (of 2020) includes provisions for e-commerce and digital services, ensuring that consumers are protected from fraudulent practices.

2. Content Moderation

Europe's Digital Services Act (DSA) sets a high standard for content moderation by mandating the swift removal of illegal content, transparency in content moderation practices, and risk assessments to combat misinformation and cyber threats. In the Asia-Pacific region, India's Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules of 2021 require platforms to remove unlawful content and increase transparency in algorithmic decision-making, while Singapore's Online Safety (Miscellaneous Amendments) Act protects users from harmful content and ensures accountability through annual reports.

In the MENA region, the UAE's Internet Access Management (IAM) Regulatory Policy monitors and restricts what the Telecommunications and Digital Government Regulatory Authority considers to be inappropriate content, including terrorism-related material and unlicensed VoIP services.

Across DCO membership, similar efforts have been made, requiring social media companies to remove harmful content and establish local offices to address grievances. An example includes Nigeria which has enacted the Cybercrimes (Prohibition, Prevention, etc.) Act of 2015, which includes provisions for content moderation and combating cyber threats.

3. Data Privacy and Security

In the U.S., states like California have enacted the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA), which grant individuals greater control over their personal data and mandate transparency in data collection practices.

Europe's General Data Protection Regulation (GDPR) takes a wide-ranging approach to data privacy, requiring platforms to handle personal data responsibly, often with a global jurisdiction. In the Asia-Pacific region, Japan's Act on the Protection of Personal Information (APPI) emphasizes user consent, data minimization, and cross-border data transfer protocols, and Singapore's Personal Data Protection Act

emphasizes transparency and accountability in data usage.

In Sub-Saharan Africa, Kenya's Data Protection Act aligns with the EU's GDPR principles, granting individuals control over their data, while South Africa's Protection of Personal Information Act (POPIA) governs data privacy and requires user consent for data collection.

In Latin America, Brazil's General Data Protection Law (LGPD) (2018) governs data privacy and protection, aligning with global standards such as the EU's GDPR.

Across DCO Member States, examples include Morocco, which has introduced data protection laws, including the Data Protection Act (2009), which regulates the processing of personal data, and Jordan, among others, which enacted a law on personal data protection. Saudi Arabia's Personal Data Protection Law (of 2023) also stands out as a key example of data privacy legislation within the DCO.

Data privacy remains a contested area with ongoing debates between regulators and tech companies. A notable example is the ongoing disagreement between the U.K. government and Apple over the implementation of end-to-end encryption. The government contends that such encryption could obstruct law enforcement efforts by limiting access to vital information during investigations, thereby posing risks to public safety. In contrast, Apple argues that strong encryption is fundamental to safeguarding user privacy. This debate highlights the complexities of balancing privacy rights with security concerns in the digital age and underscores its implications for governing a responsible digital ecosystem.

4. Competition

The EU has introduced a comprehensive framework in an effort to promote fair competition in the digital markets. The EU's Digital Markets Act (DMA) imposes a set of defined obligations on large digital platforms classified as "gatekeepers" to prevent anti-competitive behavior, ensuring a level playing field for smaller players in the digital ecosystem. Similarly, Australia has implemented the News Media Bargaining Code, which aims to address the bargaining relationship between the so-called "designated" large digital platforms, including Google and Meta and Australian news businesses. The code requires the designated platforms to compensate news organizations for content shared on their platforms. The Australian Competition and Consumer Commission (ACCC) has also been making efforts to govern the digital platforms to enhance competition and consumer protection.

In Asia, China's Anti-Monopoly Guidelines for the Platform Economy (of 2021) provide tailored guidance on competition laws, focusing on user data collection, platform classification systems, and unfair online practices.

Among DCO Member States, Saudi Arabia has developed regulatory frameworks to foster a competitive digital content market through its Regulations on Providing Digital Content Platform Services (of 2023). Among other things, these regulations focus on market development and competitiveness. Other DCO Member States have also taken steps to promote competition in digital platforms. For example, Bahrain updated its Competition Promotion and Protection Law in 2018, including new rules to target anti-competitive practices in digital markets.

The regulatory efforts across the globe reflect a growing recognition of the need to balance innovation with accountability, ensuring that digital platforms operate in ways that benefit society while supporting the health and sustainability of digital ecosystems.

2.6 Efforts by Global Digital Platforms

Complementing these regulatory efforts, major digital platform providers are also taking proactive steps to promote a responsible digital ecosystem. These initiatives reflect a growing recognition of the need for self-regulation and ethical practices within the industry. However, challenges such as misinformation, algorithmic bias, and data privacy concerns persist. Below are recent examples of initiatives by leading platforms:

Meta: Meta has announced the launch of a new digital literacy program for middle schoolers, which aims to highlight the possible dangers of online interaction, and how kids can recognize grooming, sextortion scams, and other types of online exploitation, both in its apps and across the web more broadly. The company has also introduced transparency features, such as ad libraries, to provide users with insights into political advertising.

WeChat: As a super-app, WeChat has implemented strict content moderation policies, including the disclosure of AI-generated content, to comply with Chinese regulations.

Amazon: Amazon has focused on combating counterfeit products and has pledged to ensure fair competition on its online retail platforms.

Apple: Apple has prioritized user privacy with features like App Tracking Transparency, which allows users to control how their data is shared. The company also enforces strict guidelines for apps on its App Store to ensure safety and quality.

Grab: As one of Southeast Asia's leading ride-hailing and delivery platform, Grab has introduced safety features for users and drivers, including real-time tracking and emergency assistance. Grab promotes financial inclusion by offering various financial products specifically designed for gig-workers, including emergency cash loans and product-based loans.

2.7 Key Challenges and Opportunities

While both policymakers and platforms are making strides, significant challenges and opportunities remain in ensuring the responsible governance of the digital ecosystem.

Key Opportunities

1. **Global and Regional Cooperation on Digital Governance:** Strengthening international coordination on digital regulations can reduce compliance burdens and foster responsible innovation. Initiatives like the G20 Digital Economy Working Group, the Organization for Economic Co-operation and Development (OECD) AI Principles, and DCO-led collaborations provide platforms for harmonizing policies on data privacy, AI ethics, and digital competition. Establishing common frameworks, such as interoperable data protection standards or cross-border AI governance mechanisms, can create a more predictable and trustworthy digital environment.

2. **Advancing Technology Governance for Trust and Safety:** Responsible AI development and data governance can enhance transparency, accountability, and trust in digital platforms. Governments and industry leaders can implement AI ethics guidelines, conduct algorithmic audits, and require explainability in automated decision-making to mitigate bias and discrimination. Additionally, privacy-enhancing technologies such as differential privacy and federated learning can enable data-driven innovation while safeguarding user rights.

3. **Promoting Inclusive and Sustainable Digital Ecosystems:** Governments, businesses, and civil society can collaborate to expand digital inclusion initiatives by investing in infrastructure, promoting affordable internet access, and integrating digital literacy programs into national education systems.

Encouraging accessibility standards—such as the Web Content Accessibility Guidelines (WCAG)—ensures that digital services are usable by all. Furthermore, adopting sustainable digital practices, including green data centers and circular economy models for e-waste management, can align digital transformation with environmental responsibility.

Key Challenges

1. **Regulatory Fragmentation and Compliance Burdens:** Governments worldwide are adopting diverse regulatory approaches to digital governance, creating a fragmented landscape that complicates compliance for businesses operating across multiple jurisdictions. Variations in data protection laws (e.g., GDPR in Europe vs. sectoral regulations in the U.S.), AI governance frameworks, and content moderation policies lead to inconsistencies that hinder global cooperation. The lack of regulatory alignment also creates barriers for smaller enterprises that lack the resources to navigate complex compliance requirements.

2. **Balancing Platform Accountability with Free Expression:** Digital platforms face increasing pressure to mitigate harmful content, misinformation, and cyber threats while preserving freedom of expression. Striking this balance remains challenging, as automated moderation tools often fail to consider cultural and linguistic nuances, leading to over enforcement or under enforcement of content rules. At the same time, regulatory interventions—such as requirements for proactive content removal risk undermining democratic discourse if not carefully implemented with safeguards for transparency and due process.

3. **Digital Inequality and Barriers to Access:** Despite rapid digitalization, a significant portion of the global population remains underserved due to limited internet access, high costs of digital services, and low digital literacy rates. In developing economies, infrastructure deficits exacerbate the digital divide, preventing equitable participation in the digital economy. Moreover, accessibility challenges persist for people with disabilities, older populations, and marginalized communities, further widening socio-economic disparities.

2.8 The Road Ahead

As governments, businesses, international organizations, civil society, and other stakeholders continue to shape the future of digital ecosystems, the ongoing efforts highlighted in the previous sections underscore the need for a more coordinated and forward-looking approach. The evolving digital landscape demands sustained action to address pressing governance challenges while fostering inclusive, ethical, and sustainable ecosystems. Moving forward, key emerging priorities will define the next phase of responsible digital ecosystem development, requiring deeper engagement from policymakers, industry leaders, and regulatory bodies.

Looking ahead, the fourth edition of the DCO Policy Watch will explore **three interconnected thematic areas that are essential to ensuring that digital platforms contribute to the development of a responsible digital ecosystem.** These areas reflect **core governance, ethical, and market considerations** that shape platform accountability and impact broader digital environments:

Emerging Priorities for Responsible Digital Platform Governance

1. **Online Safety and Digital Trust:** As digital platforms continue to serve as primary spaces for communication, commerce, and social engagement, ensuring user safety has become a defining issue for a responsible digital ecosystem. Trust is the foundation of a well-functioning digital ecosystem, yet platforms face increasing challenges such as cyberbullying, child exploitation, digital harassment, and algorithmic amplification of harmful content. Regulatory interventions—such as the U.K.'s Online Safety Act and the EU's Digital Services Act—are shaping new responsibilities for platforms in mitigating these harms while upholding fundamental rights. Future discussions will examine how platforms, regulators, and digital infrastructure providers can collaboratively ensure safety in a way that maintains trust and integrity within the broader ecosystem.

2. **Content Governance and Platform Accountability:** The rise of user-generated content and AI-driven content distribution has placed immense pressure on platforms to moderate effectively while ensuring fairness, accuracy, and inclusivity. A responsible digital ecosystem requires governance models that balance platform autonomy with accountability, ensuring content moderation is transparent, consistent, and fair across digital spaces. Existing moderation approaches—such as automated filtering, human review, and community flagging—remain imperfect, leading to concerns over bias, over enforcement, and censorship. This edition of the DCO Policy Watch will explore the best practices in content governance, including multi-stakeholder governance frameworks, independent oversight bodies, and regulatory mechanisms that promote trust and transparency across the digital ecosystem.

3. **Fair Competition and Sustainable Digital Markets:** Digital platforms function as marketplaces, communication channels, and economic enablers, yet their increasing dominance in key sectors has raised concerns about market concentration, anti-competitive behavior, and systemic risks to smaller innovators and startups. A responsible digital ecosystem must ensure a fair, open, and competitive digital market that fosters innovation, prevents abuse of market power, and supports interoperability between services. Regulatory interventions such as the EU's Digital Markets Act and antitrust actions in the U.S. seek to address platform gatekeeping, self-preferencing, and unfair data-sharing practices. Moving forward, this edition of the DCO Policy Watch will examine how regulatory frameworks are evolving to promote fair competition, encourage open ecosystems, and align platform governance with global digital market sustainability.

By addressing these priorities, DCO Member States, digital platforms, and industry stakeholders can work together to ensure that digital ecosystems are safe, fair, and accountable for all. This chapter sets the stage for deeper explorations into these challenges and opportunities, providing a foundation for understanding how digital platforms shape the responsible digital ecosystem. The upcoming chapters will offer in-depth insights for policymakers, industry leaders, and stakeholders navigating the complexities of digital governance, ensuring that digital transformation leads to a more sustainable and inclusive digital future.

3 Online Safety and Digital Trust

3.1 Overview

Building on the foundational principles of a responsible digital ecosystem outlined in the previous chapter, this chapter explores online safety as a core pillar in fostering digital trust. Online safety encompasses practices and policies designed to protect users from a range of digital risks, commonly grouped under the "4 Cs", which refer to:

1. Exposure to harmful **content,**
2. Risky **contact** with others,
3. Inappropriate or abusive **conduct,** and
4. Unsafe or exploitative **commercial** practices.

Closely linked to online safety is digital trust, defined as the confidence users place in digital platforms, technologies and providers to act securely, ethically, and responsibly. Trust is critical to the adoption of digital services and is built, in part, on strong online safety measures. Without trust, user engagement diminishes, and broader societal and economic benefits are undermined.

Embedding safety and trust in digital platforms strengthens the responsible digital ecosystem by ensuring that they are designed and deployed in ways that respect human rights. Within the responsible digital ecosystem, platforms and digital service providers develop and deploy technology in a manner that respects human rights and promotes user well-being. Online safety and trust are especially for children and the vulnerable. International principles affirm that the dignity and rights of a child to be protected from exploitation are no less important than the right to privacy, and that both must be respected, protected, and realized in digital contexts.

As of 2023, digital platforms connect over 5.4 billion people, roughly 67% of the world's population. Consequently, there is growing recognition that strong online safety measures are needed to address emerging harms. These harms include exploitation, algorithmic amplification of harmful content, and growing data privacy risks, among others. The internet has become a tool for widespread abuse, from cyberbullying and child grooming to complex scams like romance fraud, which have cost victims fortunes. These abuses often cause severe psychological, financial, and reputational harm, with some cases linked to self-harm and even suicide. Additionally, algorithms that drive engagement on social media can also amplify divisive or harmful content, including hate speech and misinformation, contributing to online radicalization and the spread of conspiracy theories, as echoed by the European Commission.

Compounding these risks, data privacy breaches and cyberattacks are on the rise, further eroding public trust in digital services. Surveys indicate that 84% of Americans express concern over how their personal data is handled on the internet.

With the increased attention given by stakeholders globally to these harms, diverse policy responses have started to take shape. While many countries initially relied on voluntary self-regulation by digital platforms, there is currently a global trend toward formal regulation and dedicated enforcement. The creation of new independent regulatory bodies, such as Australia's eSafety Commissioner, and the significant expansion of responsibilities assigned to the U.K.'s existing regulator, Ofcom, under the Online Safety Act 2023, underline this more proactive regulatory approach. Meanwhile, digital platforms have developed substantial internal frameworks, such as community standards and AI content filters, at times in partnership with civil society. That said, these measures are often criticized for being inconsistent and lacking external accountability.

As a result, global responses to online safety vary across regions. While some countries emphasize regulation, others prioritize collaboration and education:

Europe

Has advanced regulatory frameworks, including the EU's Digital Services Act and the U.K.'s Online Safety Act, which impose binding obligations on platforms.

Asia-Pacific (APAC)

Countries experiment with mixed approaches, combining hard and soft laws. One of the most recent example is Australia's introduction of an age-based social media ban through its Online Safety Amendment (Social Media Minimum Age) Act 2024.

North America

Largely relies on industry self-regulation and public-private partnerships, with some emerging legislative debates and changing government approaches in the region.

Sub-Saharan Africa

Focuses on regional policies and empowerment strategies, and MENA governments support collaborations with tech companies to enhance digital safety while also progressing in technology integration.

Latin America and the Caribbean

Prioritizes civil society engagement and public awareness, exemplified by the Ombudsman campaigns in Buenos Aires against digital violence.

At the international level, the transnational nature of online harms has prompted regulators and rights advocates to collaborate on cross-border solutions. The Global Online Safety Regulators Network, comprising nine online safety regulators, supported by many non-governmental organizations, exemplifies this effort by facilitating best practice sharing and coordinating responses to challenges such as misinformation and hate campaigns. No single actor can ensure that digital platforms implement effective safety measures; achieving online safety requires collaboration among governments, industry, academia, and civil society, balancing security objectives with fundamental rights like privacy and expression.

Let us now examine some specific online safety and trust practices across regions and sectors.

Latest Developments

The online safety and digital trust landscape has evolved rapidly in the past few years, marked by the enactment of significant regulations, precedent-setting enforcement actions, and the emergence of new policy proposals across jurisdictions. This section highlights major developments from 2023 through early 2025:

New legislation and laws

Several long-developing laws came into effect during this period marked primarily by the EU's DSA, which transitioned from legislation to implementation. In 2023, the European Commission designated 17 Very Large Online Platforms (VLOPs) and 2 Very Large Search Engines under the DSA including companies like Google, Facebook, X, TikTok, etc. subjecting them to stricter requirements. These include obligations such as enhanced transparency reporting, mandatory risk assessments, independent audits, and robust mechanisms for content moderation. For instance, platforms must now provide clear explanations regarding content recommendations and maintain accessible user appeals processes.

Strengthening global alignment with international cyber safety norms

The adoption of the U.N. Convention against Cybercrime in December 2024 has enhanced international cooperation in combating cybercrime.

Emergence of independent online safety regulators

Australia's eSafety Commissioner, first established in 2015, exercised newly granted enforcement powers to impose fines on multiple digital platforms. For instance, the encrypted messaging app Telegram was fined nearly $650,000 for failing to respond promptly to inquiries regarding its measures to combat terrorism and child abuse material on its platform.

Disinformation and war reporting

Recent developments extend beyond policy, as real-world events tested the resilience of online safety mechanisms. For instance, during recent global conflicts, digital platforms saw a surge in graphic content and propaganda, highlighting the growing challenges of disinformation and content moderation.

3.2 Regional Approaches

3.2.1 Public Sector Approaches

This section examines measures by governments through a comparative analysis of the online safety and digital trust best practices across regions including Europe, APAC, and MENA, North America, Latin America and the Caribbean (LAC), and Sub-Saharan Africa (SSA). It highlights key policy instruments shaping the digital governance landscape in these areas.

Europe

In Europe, the EU has taken a proactive approach to enhancing online safety and digital trust, particularly with the Digital Services Act (DSA), which became fully applicable in February 2024. This regulation imposes clear legal duties on digital services operating in the EU, requiring them to implement basic mechanisms such as enabling users to flag illegal content and mandating regular transparency reporting. Its goal is to create a "safe, predictable and trusted" online environment.

However, the most stringent obligations under the DSA specifically target Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs). Platforms are categorized as VLOPs if they have at least 45 million monthly active users in the EU. These larger entities face enhanced obligations, including detailed transparency regarding algorithms and content moderation processes, external audits, systemic risk assessments, dedicated measures to combat disinformation, and mandatory data access provisions for independent research purposes.

Prior to the DSA, several EU member states had enacted similar, national-level laws. Germany's Network Enforcement Act (NetzDG) (2017) was one of the first laws globally to require social media networks to swiftly remove hate speech and illegal content.

In addition to illegal content removal, the EU has initiated co-regulation and safety-by-design approaches, especially for child protection. The Audio-visual Media Services Directive (AVMSD) was revised in 2018 to extend content standards to include the protection of minors from harmful content and the prohibition of incitement to violence and hatred on video-sharing platforms.

These regulatory efforts have positioned the EU at the forefront of setting global standards in digital governance, shaping policy discussions worldwide through what is known as the "Brussels Effect." The DSA in particular has set a precedent for comprehensive digital regulation, and prompted other regions to consider similar frameworks to ensure online safety and uphold digital trust.

Case Study: Ireland's Online Safety Commissioner

Ireland established a dedicated online safety regulator ahead of the E.U.'s DSA enforcement. The Online Safety and Media Regulation Act 2022 established the Coimisiún na Meán, incorporating an Online Safety Commissioner. This office is authorized to create binding codes of practice for online services and address complaints about harmful online content. Notably, Irish residents can escalate unresolved issues to the regulator if platforms fail to remove reported harmful content. Given that many "big tech" companies have their EU headquarters in Dublin, this regulatory framework allows the Irish regulator to influence company practices globally.

The U.K.'s Online Safety Act (2023) introduces a duty of care for platforms to address both illegal and certain harmful content, with a strong focus on child protection. Ofcom, the main communications services regulator, is authorized to issue codes of practice and impose fines of up to 10% of global turnover of digital platforms in cases of non-compliance. Additionally, senior managers in tech companies may face criminal liability if they fail to comply with specific child-safety obligations. While the Act has sparked debate—particularly concerning potential privacy implications related to scanning encrypted messages—it exemplifies a detailed, accountability-focused regulatory framework for online safety.

Latin America and the Caribbean

Latin America and the Caribbean (LAC) countries are progressively addressing online harms, though their approaches differ. In 2023, Brazil debated the proposed "Fake News Law," aiming to impose transparency requirements and due diligence on social networks and messaging services to combat online falsehoods and extremism. The law sought to obligate platforms to promptly remove content involving crimes, such as threats against democracy, and demonetize purveyors of misinformation. In 2013, Argentina enacted legislation criminalizing online grooming of minors. This law was further strengthened in 2020 with the passage of "Ley Mica Ortega," named in memory of a 12-year-old victim of online grooming and murder. These initiatives reflect a growing recognition in the region of the need to address various online harms through a combination of legislation and public awareness efforts.

Case Study: Te Protejo Colombia

This Colombian program operates a hotline where people can report suspected CSAM they encounter online, allowing authorities to investigate and remove the content. The initiative has also expanded to reach 276 municipalities across Colombia, demonstrating its broad national reach.

North America

Under Section 230 of the Communications Decency Act 1996, U.S. digital platforms are largely shielded from liability for user-generated content, with exceptions for federal crimes and intellectual property violations. This legal framework has facilitated the growth of social media but has also presented challenges in addressing harmful content. Rather than implementing comprehensive federal regulations, the U.S. has focused on targeted measures. For instance, bipartisan concerns about child safety online have led to proposals like the Kids Online Safety Act (KOSA) and updates to the Children's Online Privacy Protection Act (COPPA). Additionally, the government has exerted pressure on companies through hearings and summits to adopt voluntary improvements in content moderation policies. In 2024, the Senate Judiciary Committee hosted a full committee hearing on online child sexual exploitation, demanding answers from social media companies. CEOs from those platforms, including Discord, Meta, Snap, TikTok, and X testified about their efforts in protecting children from online sexual exploitation.

Canada is moving toward more structured regulation. The Digital Charter (2019) outlines principles such as "Safety and Security" and "Strong Enforcement and Real Accountability." In 2022, the government proposed the Online Harms Bill to establish a regulator overseeing how platforms address harmful content, including terrorism, hate speech, and child exploitation. This approach aligns more closely with European models with its emphasis on proactive measures to ensure online safety.

Case Study: Canada's Project Arachnid

Project Arachnid, run by the Canadian Centre for Child Protection (a charity), while not a law or policy, is a technological and collaborative solution that has become a global best practice for tackling Child Sexual Abuse Material (CSAM). It is a web-crawling system that continuously scans billions of images and videos on the internet for known child abuse imagery, using hashes and other detection methods. When it finds a match or probable CSAM, it automatically sends a notice to the host or service provider to remove the content.

Asia-Pacific (APAC)

The APAC region exhibits diverse approaches to online safety, ranging from emphasizing independent oversight and cooperation between stakeholders, as seen in countries like Australia and Singapore, to more state-controlled frameworks prioritizing government oversight and stricter content moderation measures, surveillance measures, and user identification requirements.

Australia established the world's first eSafety Commissioner in 2015, further strengthening its commitment with the Online Safety Act 2021. This Act empowers the Commissioner to enforce rapid removal of harmful content and set safety expectations for online services.

In 2022, Singapore enacted the Online Safety (Miscellaneous Amendments) Act, requiring large social media platforms to implement measures against explicit content. The Infocomm Media Development Authority (IMDA) can direct platforms to disable access to harmful content which enforces an industry code of practice on online safety.

South Korea has implemented measures to combat cyberbullying, reflecting a proactive stance on online safety. The government has announced new anti-bullying laws aimed at addressing these issues. It also recognizes cyberbullying as a form of school violence and provides support mechanisms for victims. Vietnam has enacted "Decree 147", a social media regulation that mandates users to verify their accounts with phone numbers or national ID cards, reflecting a more state-controlled approach to online safety.

In 2021, India introduced the Information Technology Rules (Intermediary Guidelines and Digital Media Ethics Code), which mandate that social media intermediaries appoint compliance officers and proactively address grievances related to harmful content. The rules classify platforms exceeding a specified number of users as Significant Social Media Intermediaries, which must comply with additional obligations.

New Zealand illustrates a balanced approach with initiatives like Netsafe, a non-profit organization that provides online safety education and assistance, and the Harmful Digital Communications Act 2015, a law designed to combat cyberbullying and online harassment by providing mechanisms for addressing online abuse, including court orders.

Case Study: Singapore's "Mystery Shopper" Online Safety Audit

Singapore has implemented a regulatory practice consisting of auditing social media platforms' responsiveness using "mystery shopper" techniques. After the new Code of Practice came into effect, IMDA conducted an Online Safety Assessment Report (2024) where analysts posed as regular users and filed over 1,000 reports of harmful content across six major platforms. The findings highlighted that more than half of the legitimate user complaints were not addressed by the platforms on the first attempt. In many cases, harmful posts stayed up until IMDA officially notified the platform. On average, most companies took five days or more to act on user reports slower than the response times they advertised in transparency reports.

Middle East and North Africa

Several MENA states have recently implemented initiatives to enhance online safety, focusing on education, regulation, and collaboration.

In Bahrain, the National Cyber Security Centre launched the "Cyber Aware Bahrain" campaign in 2023, which aims to raise cybersecurity awareness among children and parents, addressing risks such as online exploitation and blackmail. The campaign underscores a collective responsibility to foster a secure digital environment.

In the UAE, Federal Decree-Law No. 34 of 2021 on Combatting Rumors and Cybercrimes applies to digital content. The list of crimes includes insult and slande, child pornography; or propagating terrorist groups. Moreover, Federal Law No. 3 of 2016 on Child Rights Law (Wadeema's Law) aims to protect children's data online and mandates the reporting of child pornography as well as information on persons, bodies, or websites that exchange such materials or intend to mislead children. The country established the Digital Wellbeing Council in 2019 to promote digital literacy and responsible internet use. In 2025, the UAE introduced the Children's Digital Wellbeing Pact, a collaborative effort involving government bodies and tech companies like Snapchat, Google, and Meta. The pact focuses on creating a safer online environment for children by enhancing their digital literacy and protecting them against harmful content.

In Saudi Arabia, the Anti-Cyber Crime Law (2007) criminalizes online defamation, identity theft, and privacy violations, serving as a deterrent against cyber harassment. Additionally, authorities and non-profits have conducted campaigns promoting respectful internet use and cautioning against cyberbullying. For instance, in September 2023, the Ministry of Health launched an anti-bullying awareness campaign in schools, aiming to enhance students' mental health by reducing bullying incidents.

Egypt's ICT Ministry, alongside the Egyptian National Council for Childhood and Motherhood and UNICEF, launched the Internet Safety Campaign in December 2024. That same month, the ICT Ministry, the Directorate of Education, and UNICEF organized the Child Online Protection Program. In March 2022, the Moroccan Ministry of Justice, in partnership with the Moroccan Centre for Polytechnic Research and Innovation (CMRPI), organized the Technical Workshop on Child Protection Online, aimed at developing concrete recommendations to improve the legal framework for the protection of minors online in Morocco.

Case Study: Salam@ ("Salamat")

Salam@ is an initiative by The SecDev Foundation aimed at enhancing digital safety for women and youth across the MENA region. It employs a public health approach to digital resilience, providing resources such as research publications, digital safety guides, and a sign-language dictionary to empower communities against digital threats. Salam@ ("Salamat") helps MENA women use new digital technologies to improve their online experiences and protect themselves from hacking, harassment, scams, blackmail, theft, and other digital harms. The team is pioneering a public health approach to digital violence, integrating prevention, frontline intervention, public awareness, and policy advocacy, supported by evidence-based research.

Sub-Saharan Africa

The countries in the SSA region are increasingly implementing legal frameworks to enhance online safety. For instance, Kenya's Computer Misuse and Cybercrimes Act criminalizes offenses such as cyber harassment, false publications, and child pornography, facilitating the prosecution of cybercrimes. Ghana has also implemented a Child Online Protection Framework (2021–2025), in collaboration with UNICEF and International Telecommunication Union (ITU), which includes school curricula on online safety and tighter enforcement against cybersex trafficking.

On a continental scale, the African Union's (AU) Convention on Cyber Security and Personal Data Protection obliges member states to criminalize online child abuse, racism, and xenophobia, and to enhance user data privacy. Additionally, several African countries, including Nigeria, South Africa, Kenya, Rwanda, and Senegal, are members of the Global Alliance to Counter Child Sexual Abuse Online (WeProtect), as they commit to national action plans for child online safety.

As seen with the above examples, the following are likely to take priority in the region:

- Adoption of regional frameworks under the African Union's Digital Transformation Strategy.
- Initiatives to improve digital literacy among users.
- Partnerships with global organizations to address cybercrime and misinformation.

Case Study: African Union Child Online Safety and Empowerment Policy

The AU's policy is a landmark practice in regional cooperation for online safety. The policy is comprehensive: it calls for member states to review and update their laws to address online child abuse and exploitation, to train law enforcement and the judiciary in handling cyber cases, to encourage tech companies to build safety into products, and to invest in education and awareness campaigns for children, parents, and teachers.

3.2.2 Private Sector/Self-Regulation

Large digital platforms have implemented specific initiatives to enhance online safety and digital trust:

- Google developed Safe Browsing, a technology that alerts users attempting to visit dangerous websites.
- Meta collaborated with Childhelp to create a curriculum aimed at teaching middle school students how to detect online exploitation forms like sextortion and grooming.
- TikTok partnered with the Family Online Safety Institute to develop a Digital Safety Partnership for Families, designed to help families start conversations about online experiences and set positive digital boundaries together.
- Google, OpenAI, Roblox, and Discord launched ROOST (Robust Open Online Safety Tools), a non-profit organization providing free, open-source AI tools to detect and report CSAM, aiming to enhance child safety online.

DCO Landscape

Collectively, DCO's Member States have launched collaborations that underscore online safety and digital trust, such as the DCO Digital Rights Intent on Safe Digital Space for Children, adopted during the DCO's 4th General Assembly in February 2025. Below are some examples of each Member State's national approach and any joint DCO initiatives on these issues:

Member State	Key Initiatives and Strategies
Bahrain	Bahrain has implemented multiple measures to ensure online safety. The Kingdom's Law No. 60 of 2014 on Information Technology Crimes criminalizes online offenses such as hacking and the distribution of illegal content including child pornography. In 2023, it launched a national cybersecurity awareness campaign to educate parents and children about risks like online exploitation and cyberbullying. The Telecommunications Regulatory Authority (TRA) has run Child Online Protection training for educators, and Bahrain operates a 24/7 Child Helpline (998) for reporting online (and offline) abuse. The National Strategy for Childhood 2023–2027 also emphasizes protecting children in the digital environment. Additionally, the Constitution of Bahrain (2002) contains provisions on data protection and privacy, with a focus on confidentiality of communications including electronic communications.
Bangladesh	Bangladesh has been reforming its digital policy framework. In 2023, it repealed the Digital Security Act 2018 and replaced it with a new Cyber Security Act. This law punishes the dissemination of false or defamatory information, online harassment, and cyber fraud, while also retaining strict penalties for CSAM. Bangladesh has also set up various specialized cybercrime police stations. A cyber incident Response Unit, Cybercrime Investigation Cell, and 'IT Crime Forensic Lab' have been established by the Bangladesh Police to fight against cybercrime or crimes related to computers and other IT technologies.
Cyprus	As an EU member, Cyprus adheres to the EU's digital regulations like the DSA and GDPR. Cyprus Law No. 22 (III) ratifies the Budapest Convention on Cybercrime and providesfor the criminalization of cybercrimes such as hacking, child pornography, internet fraud and fraud through electronic communications. Law 91(I)/2014, titled "The Prevention and Combating of Sexual Abuse and Sexual Exploitation of Children and Child Pornography Law," aims to prevent, suppress, and combat child sexual abuse, exploitation, and child pornography. The Cyprus Safer Internet Center, supported by the European Commission, is a focal point for awareness, helpline, and hotline services dealing with online safety issues. Its national police has a cybercrime unit that cooperates with INTERPOL operations against online child abuse. With relatively high internet penetration, Cyprus emphasizes digital literacy, with the Ministry of Education integrating e-safety into curricula.
Djibouti	Djibouti's online safety framework is reflected in Law No. 66/AN/14/7ème on Cyber Security and the Fight Against Cybercrime (2014). This law criminalizes unauthorized access to systems, data breaches, online fraud, and bans child pornography. Specific legislation on cybercrime has also been enacted through Articles 548-555 of the Penal Code on computer-related offenses, prescribing crimes such as illegal access, illegal interception, data interference, system interference and computer related fraud, along with the corresponding penalties.

Member State	Key Initiatives and Strategies
Gambia	The 2013 amendment to the Information and Communications Act – which imposed heavy penalties for false news online – was declared unconstitutional and abandoned in 2017. Currently, the Information and Communications Act (2009) and Criminal Code are used to address online offenses – e.g. there are penalties for hacking, spreading false information, and obscenity online. The Gambia also introduced a Cybercrime Bill in 2023-2024. To promote trust, the Gambia launched an initiative to establish a national Computer Security and Incident Response Team (CSIRT) with a focus on protecting critical systems and the public from cyber threats.
Ghana	Ghana's Cybersecurity Act is a law that established the Cyber Security Authority (CSA) and comprehensively addresses online crimes and security. Under this Act, Ghana has taken steps such as launching a Cybercrime/Cybersecurity Incident Reporting Points of Contact (PoC) for the public and requiring major digital service providers to register with the CSA and implement measures against crimes like cyberstalking and online fraud. Ghana has also implemented a Child Online Protection Framework (2021–2025), in collaboration with UNICEF and ITU, which includes school curricula on online safety and tighter enforcement against cybersex trafficking.
Greece	Greece, as an EU member, aligns with the EU's regulatory standards for online safety. In 2021, it amended the Criminal Code to criminalize the spreading fake news that could cause public fear or undermine public order or public health, with penalties of up to five years' imprisonment. Nationally, Greece set up the SafeLine hotline for reporting illegal internet content and the Greek Safer Internet Center which raises awareness about responsible and better use of the internet and mobile technologies among children and young people. In late 2024, Greece launched a National Strategy for the Protection of Minors Online, introducing new digital tools for parental controls and age verification. This includes a forthcoming "Kids Wallet" system to help verify users' ages and limit underage social media use, as part of broader efforts to tackle internet addiction, cyberbullying, and exposure to harmful content among youth.
Jordan	Jordan's approach to online safety recently took a stronger turn with the Cybercrimes Law No.17 of 2023. Law 17/2023 includes the following: definitions (Article 2), illegal access (Article 3), illegal access to public institution network and information systems (Article 4), forgery (Article 5), system interference (Article 6), unlawful interception (Article 7), fraud (Article 8, 9, 10), misuse of devices (Article 11), pornography cybercrime (Article 13), and slander and denigration (Article 15, 16, 20). Articles 14, 17, 18 and 19 include provisions that are not envisaged in the Budapest Convention. Beyond legislation, Jordan has undertaken public initiatives for digital safety: a recent UNICEF-supported campaign dubbed "Not Right" delivered school lectures and media messages about preventing child sexual exploitation.

Member State	Key Initiatives and Strategies
Kuwait	Several Kuwaiti laws provide a basis for prosecuting cybercrime. These laws include • Law No. 63 of 2015 Regarding Anti-Information Technology Crime, • Law No. 37 of 2014 Regarding the Establishment of the Communications and Information Technology Regulatory Authority, • Law No. 20 of 2014 Regarding Electronic Transactions, • Law No. 9 of 2001 Regarding Misuse of Telecommunications and Wiretap Sets, and • Law No. 16 of 1960 Promulgating the Penal Code.
Morocco	Morocco has steadily built a legal framework on cyber issues. Morocco promulgated Law 103.13 on Combating Violence Against Women in 2018. An important aspect of the new law was that Article 503(1)(1) of the Moroccan Penal Code expanded the definition of sexual harassment to include written messages by phone or any other electronic device, recordings, and the procurement or creation of images of a sexual nature for sexual purposes. Article 447(2) of the law also criminalizes the distribution of another person's messages and photos without prior consent and the dissemination of false allegations aimed at harming or defaming someone's private life by any means, including digital tools.(27) Its 2018 National Cybersecurity Strategy emphasizes securing digital infrastructure and nurturing trust to support its digital economy ambitions. The National Commission for the Control of the Protection of Personal Data (CNDP), runs a program called "Data-Tika" which not only enforces privacy laws but also promotes a culture of respecting users' personal data – seen as a pillar of digital trust.
Nigeria	Nigeria's Cybercrime Act criminalizes a range of online harms including identity theft, cyberstalking, revenge porn,and more and has been actively used. In 2023, Nigeria approved a dedicated National Child Online Protection Policy and Strategy to coordinate efforts to safeguard children on the internet. Under this policy, government agencies led by the Ministry of Communications and Digital Economy and the telecommunications regulator are working alongside schools and NGOs to educate young users, filter harmful content, and improve the reporting of online child exploitation.
Oman	The Omani Penal Code and a Cybercrime Law collectively cover online offenses – punishing hacking, online fraud, defamation, and public morals violations online. The Cybercrime Law 2011 contains substantive provisions on violations of safety, confidentiality of data and electronic information and the informational systems; including • Illegal access, data interference, system interference (Articles 3-10), (Chapter Two); • Misuse of information technology tools (Article 11), (Chapter Three); • Computer-related forgery and computer-related fraud (Articles 12 and 13), (Chapter Four); • Content-related crimes, further prescribed in (Chapter Five) of the law. To promote trust, Oman established a National Cyber Defence Centre in 2020, which defends government networks and acts on cyber incidents affecting businesses and individuals (e.g. major phishing campaigns). Oman has also joined the WePROTECT Global Alliance to fight child exploitation.

Member State	Key Initiatives and Strategies
Pakistan	The Prevention of Electronic Crimes Act (PECA) 2016 is Pakistan's primary cyber law, which criminalizes online harassment, hate speech, impersonation, and other offenses. It also gives the Pakistan Telecommunication Authority (PTA) powers to block content deemed indecent, immoral, or a security threat. In addition to enforcement under the Act, authorities have launched cyber safety awareness campaigns and established a Cyber Crime Wing under the Federal Investigation Agency (FIA) to investigate offenses and support victims, reflecting a growing emphasis on digital trust and security.
Qatar	Qatar has rapidly advanced its digital infrastructure and is correspondingly building safety and trust measures. It has a Cybercrime Prevention Law 2014 that prohibits hacking, phishing, and the online spreading of false news or defamation. In terms of child safety, Qatar has a portal called "Safe Space" which caters to young people, caregivers, children, educators, and the public. It is equipped with information and resources on cyber safety and security, provides educational games and tips, and offers up-to-date insights on cyberbullying to help parents and teachers protect children against such threats. At the community level, Qatar has supported digital literacy initiatives like Vodafone's "AmanTECH" program, which educates children, parents, and teachers about safe internet use and cyberbullying prevention.
Rwanda	Law No. 60/2018 on the Prevention and Punishment of Cyber Crimes covers crimes such as unauthorized access, data interception, and computer fraud, and bans the online dissemination of harmful or illegal content. Rwanda's cybersecurity strategy involves a centralized National Cyber Security Authority (NCSA), which conducts awareness programs such as the annual Cybersecurity Week targeting the public with tips on safe internet practices. In addition, the Rwanda Child Online Protection Policy ("the COP Policy") is designed to mitigate risks and harms against children, and to provide a framework that meets children's needs and fulfills their rights, while enabling them to safely and confidently navigate the digital environment.
Saudi Arabia	Saudi Arabia has made digital trust and safety a core part of its national economic diversification and digital transformation strategy (Vision 2030). The Kingdom's approach involves a mix of regulatory enforcement and initiatives to build trust in emerging technologies. On the regulatory side, Saudi Arabia's Anti-Cyber Crime Law (2007) criminalizes online offenses such as defamation, hacking, and the production or distribution of pornographic materials. In recent years, the Kingdom introduced new regulations specifically targeting the digital sphere: in 2022–2023 the Communications, Space & Technology Commission (CST) proposed a "Global Digital Content Trust" framework (also refered to as the Safe Harbor Law) to clarify platforms' liability when hosting user content. It also issued the Regulations for Providing Digital Content Platform Services requiring platform registration and local representation to increase platform accountability. Beyond laws, Saudi Arabia invests heavily in cybersecurity and safety technologies: the National Cybersecurity Authority runs programs for government and critical sectors, and Saudi companies are developing AI-based tools to detect extremist or terrorist content.

3.3 Road Ahead

As we progress through 2025, platform governance within digital ecosystems will continue to evolve in response to emerging threats, regulatory shifts, and technological advancements. Ensuring online safety and digital trust will increasingly depend on the ability of governments and platform providers to implement proactive governance frameworks that balance innovation with security.

The progress of Artificial Intelligence (AI) has introduced new challenges, notably the rise of AI-generated synthetic content. The Internet Watch Foundation reported over 20,000 AI-generated child exploitation images circulating on dark web fora within a single month in 2023, underscoring the critical need for digital platforms to strengthen user protection and content moderation policies, and governments to enhance regulatory oversight. Additionally, AI-driven cyber threats are becoming more sophisticated, placing new pressures on platforms to implement stronger cybersecurity measures. The World Economic Forum's Global Cybersecurity Outlook highlights that sectors such as healthcare, finance, and energy are particularly vulnerable, further demonstrating the importance of robust platform security policies within digital ecosystems.

In response to these challenges, governments worldwide are introducing regulations specifically aimed at enhancing platform accountability. The EU is advancing the proposal of the Digital Fairness Act, targeting deceptive design practices and dark patterns, with public consultations scheduled for spring 2025. In the U.K., the government is working on a new law, the Data (Use and Access) Bill (DUA), which will compel digital platforms to provide researchers with access to data so they can independently study online safety trends. According to the U.K. government, this initiative will increase transparency on the scale of online harms and the effectiveness of interventions, reinforcing platform accountability as a core component of digital trust.

As these regulatory and policy efforts take shape, effective platform governance will require deeper collaboration between governments, technology companies, and civil society. The road ahead is not just about balancing innovation with safety, it is about ensuring that digital platforms remain accountable, digital ecosystems function securely, and regulatory frameworks keep pace with technological change. With AI and cyber threats evolving at an unprecedented rate, proactive governance mechanisms and international cooperation will be essential to safeguarding platform integrity and public trust in the years to come.

Upcoming events

Web Summit Rio
April 27-30, 2025, Rio de Janeiro, Brazil

Find out more

IPPPRI25: Tackling online harms: Research into Practice
May 19-21, 2025, London, U.K.

Find out more

Safer Internet Day
February 10, 2026, 170 countries worldwide

Find out more

4 Content Governance and Platform Accountability

4.1 Overview

Ensuring online safety is not the only critical aspect of a responsible digital ecosystem. Equally important is how platforms govern content—balancing moderation with transparency, accountability, and user rights. The expansion of User-Generated Content (UGC) and AI-driven content distribution has transformed how information is created, shared, and consumed, with digital platforms serving as key enablers of this shift. While these advancements have empowered users by democratizing content production and enabling global connectivity, they have also introduced significant challenges in content governance: the policies, processes, and mechanisms that platforms use to regulate online spaces. In an increasingly interconnected digital world, ensuring that content governance frameworks uphold principles of fairness, transparency, accountability, and inclusivity is both a technical and ethical imperative.

At the heart of this issue is platform accountability, the obligation of digital platforms to implement and enforce content policies in a manner that is transparent, unbiased, and aligned with public interest values. Within digital ecosystems, platforms play a critical role in content governance by moderating online interactions and balancing freedom of expression with harm mitigation.

Striking the right balance between freedom of expression and harm mitigation remains a central challenge. Platforms are tasked with both protecting users' rights to express opinions and preventing the spread of harmful content, including misinformation, hate speech, extremism, and harassment. This tension has sparked global debates over censorship, content regulation, and the broader role of digital platforms in shaping public discourse.

In recent years, to manage these challenges, platforms have employed a range of content moderation strategies, including:

- Automated filtering powered by Machine Learning and Natural Language Processing (NLP) to detect and remove harmful content at scale.
- Human review, where moderation teams manually assess content for violations based on platform policies and community guidelines to determine whether posts should remain or be removed.
- Community reporting, in which users report content they believe violates platform rules, prompting further evaluation by automated or human moderators.

Despite their widespread use and benefits, these moderation methods present governance challenges. Algorithmic bias can lead automated systems to disproportionately target certain

communities, while over-enforcement of moderation rules can result in wrongful removals and suppression of legitimate content. Conversely, under-enforcement can allow harmful material to persist, undermining user safety and trust. Human moderators, though essential, often struggle with inconsistency and decision fatigue, leading to subjective enforcement. Moreover, community flagging systems can be exploited for mass reporting campaigns aimed at silencing certain voices. These shortcomings highlight the need for more transparent, accountable, and inclusive governance models.

Generative AI has also emerged as both an opportunity and a challenge for content governance. While it enables rapid content creation at scale, it also raises concerns about bias, misinformation, and ethical usage. The EU's AI Act, the first-ever legal framework on AI, which entered into force in August 2024 (and will be fully applicable in August 2026). It provides a blueprint for balancing innovation with accountability by emphasizing ethics and transparency. Globally, 69% of organizations are delaying AI investment decisions due to anticipated regulatory changes. This highlights the need for clear guidelines that foster readiness while addressing societal concerns about AI's impact on content governance and platform accountability.

In response to these challenges, effective platform governance requires models that balance autonomy with accountability. A growing consensus among researchers, policymakers, and digital rights advocates suggests that addressing these challenges requires multi-stakeholder governance. This model entrusts governments, tech companies, civil society organizations, independent oversight bodies, and users to collaborate in developing fair and effective content governance frameworks. Regulatory mechanisms also play a key role in ensuring accountability, with various legislative approaches emerging worldwide to hold digital platforms responsible for their moderation decisions. For instance, the EU's DSA and proposals like the U.S. Platform Accountability and Transparency Act set new benchmarks for accountability by mandating clear reporting structures, appeals processes, and algorithmic transparency.

This section explores various facets of content governance and platform accountability, emphasizing the role of multi-stakeholder frameworks, independent oversight bodies, and regulatory mechanisms. By examining these components, this chapter delineates pathways toward strengthening platform accountability within digital ecosystems, ensuring that digital services operate transparently, fairly, and in alignment with societal values.

4.2 Latest Developments

The landscape of content governance and platform regulation has evolved significantly in 2025, driven by the advancement of AI, the need for ethical frameworks, and increasing regulatory scrutiny. Governments, multilateral organizations, and private entities are introducing new policies and frameworks to address challenges such as misinformation, intellectual property rights, and ethical AI usage.

Multilateral Frameworks

The DCO concluded its 4th General Assembly in February 2025 with several landmark initiatives aimed at advancing global digital maturity. Member States endorsed efforts to develop frameworks such as the Framework for Strengthening National Agendas to Combat Online Misinformation, and the DCO Digital Rights Intent on Digital Intellectual Property Protection. These initiatives reflect DCO's commitment to fostering a human-centric digital economy that prioritizes inclusivity, transparency, and sustainability.

The Framework for Strengthening National Agendas to Combat Online Misinformation was particularly significant. Chaired by Kuwait through a Ministerial Committee, this initiative emphasizes cross-border collaboration to address misinformation while respecting cultural diversity. This builds upon previous DCO efforts in this area, including the DCO 2024 joint statement on Misinformation and the Role of Social Media Platforms and the DCO 2023 White Paper on Online Misinformation on Social Media Platforms.

Similarly, the Joint Inspection Unit (JIU) of the UN system has identified gaps in existing accountability frameworks that may reduce their effectiveness. To address these issues, the JIU recommends that UN system organizations ensure comprehensive oversight of their accountability frameworks and regularly report on their implementation to legislative organs and governing bodies. Beyond state-led governance, international economic and policy organizations, such as the OECD, have focused on algorithmic transparency and AI governance in content moderation. The OECD AI Principles, adopted by 46 countries, provide guidelines for ethical AI deployment, with a particular emphasis on ensuring fairness in automated content curation and moderation.

While these initiatives establish important normative frameworks, their reliance on non-binding agreements and voluntary commitments raises question about their real-world impact. This may lead to companies adopting cosmetic compliance strategies without making substantive changes to their moderation policies.

EU: Advancing Platform Accountability

The EU continues to lead global efforts in platform regulation through its Digital Services Act (DSA) and Digital Markets Act (DMA). These laws mandate transparency in content moderation practices, algorithmic accountability, and risk assessments for systemic harms like disinformation. Recent enforcement actions by national Digital Services Coordinators (DSCs) have revealed gaps in compliance among platforms operating across Member States.

For instance, Ireland's DSC initiated investigations into VLOPs' illegal content reporting mechanisms in early 2025, and findings highlighted inconsistencies in how moderation policies were applied across jurisdictions. These actions underscore the challenges of implementing uniform regulations but demonstrate progress toward greater accountability.

Civil society organizations have welcomed these measures as necessary steps towards a safer digital environment but caution against overreach during crises. Meanwhile, tech companies have expressed concerns about compliance costs and regulatory complexity.

The U.K.: AI Regulations and Content Governance

In January 2025, the U.K. government launched a consultation to reform copyright laws in response to the growing influence of AI. This initiative seeks to clarify how copyrighted content can be used in AI training while balancing the rights of creators and fostering innovation. One of the most controversial aspects is the proposal to allow AI developers to use online content without explicit permission. Prominent artists like Paul McCartney and Elton John have criticized this measure, arguing it undermines creators' ownership and revenue streams.

In addition to copyright reforms, the U.K. government announced broader legislative plans for AI regulation during the recent King's Speech. These plans include new laws addressing AI accountability, transparency, and ethical usage. The government aims to ensure that AI applications align with societal values while addressing concerns about bias and misuse.

Stakeholder reactions have been mixed. Technology companies welcome a clearer regulatory framework that fosters innovation but express concerns about potential restrictions on data usage. Meanwhile, content creators fear revenue losses and reduced control over their intellectual property. The government has emphasized ongoing public consultations to address these concerns.

The U.S.: Tech Companies Reassessing Content Policies

As the re-election of Trump has intensified debates on digital media regulation, concerns about misinformation and platform accountability are coming to the fore. Recent shifts in platform policies reflect a broader trend of reassessing moderation strategies. For instance, Meta has moved away from third-party fact-checking towards a community-driven approach, similar to X's model. This change is intended to align the company's strategy with CEO Mark Zuckerberg's goal of promoting free expression while reducing direct company involvement in content oversight. Meanwhile, traditional broadcasters and media outlets are advocating for regulations that promote content from trusted sources to prevent what they term an "American news swamp."

Additionally, many global platforms, including Meta, X, and YouTube, have introduced transparency reports, detailing content takedowns and moderation practices, in response to international advocacy and regulatory pressure. A study by Gillespie highlights that these measures, though imperfect, have contributed to greater public scrutiny of platform governance, leading to some policy adjustments in response to criticism.

4.3 Regional Approaches

Governments and regulatory bodies in different regions have developed varied approaches to content governance and platform accountability. While common challenges such as misinformation, hate speech, extremist content, online harassment, and algorithmic bias are universal, responses vary significantly based on legal traditions, political systems, socio-cultural norms, and economic priorities.

Some regions, particularly Europe, have pursued comprehensive regulatory oversight aimed at enforcing platform accountability through transparency mandates and liability frameworks. In contrast, in North America, the U.S. has maintained a strong commitment to free speech principles, limiting government intervention in platform regulation while debating reforms to platform immunity. The Asia-Pacific region presents a highly fragmented approach, with countries like Australia and Japan favoring platform regulation, while China and other states employ strict state-controlled censorship models. MENA and SSA grapple with state control versus digital rights advocacy, often navigating content governance in politically charged environments. Finally, LAC has taken a mixed approach, with some countries pursuing progressive regulatory policies inspired by European models, while others must first address political stability, institutional enforcement, and government-driven digital censorship.

Europe

The EU has positioned itself at the forefront of digital platform regulation through some of the most extensive and enforceable regulations on platform accountability and content governance. Its legislative approach prioritizes systemic

risk mitigation, platform transparency, and consumer protection, reflecting a broader commitment to digital rights.

The DSA represents a landmark policy requiring large online platforms to mitigate risks associated with illegal content, disinformation, and algorithmic amplification of harmful content. It mandates transparency in content moderation, imposes independent auditing mechanisms, and sets penalties of up to 6% of a company's global revenue for non-compliance, with mechanisms such as the Appeals Center Europe allowing users to challenge content decisions. The Appeals Center, based in Dublin, serves as an out of-court dispute settlement body, aiming to enhance user rights and transparency in content moderation.

Similarly, the GDPR, while primarily a data protection framework, has shaped platform governance by enforcing stricter controls on data-driven content curation and targeted advertising. The U.K. complements these efforts with its Online Safety Act (OSA), which emphasizes protecting minors from harmful content. Particularly, the OSA extends the EU's regulatory ethos by establishing criminal liability for platforms failing to remove harmful content. The law empowers Ofcom to levy fines, enforce transparency measures, and introduces criminal liability for senior executives who fail to comply with regulatory requirements.

Stakeholder reactions have been mixed. Civil society organizations have welcomed these frameworks but expressed concerns about potential overreach during crises. Tech companies have raised issues regarding compliance costs and regulatory complexity, while users have cautiously supported the measures but remain concerned about algorithmic transparency and privacy risks.

Case Study: Ireland's DSC Investigations into VLOPS

A notable case study involves the enforcement of the DSA in Ireland. In 2024, Ireland's DSC launched investigations into compliance by VLOPs. Early findings revealed inconsistencies in how platforms applied moderation policies across EU Member States – highlighting both progress toward accountability and challenges in ensuring uniform application of regulations. Nonetheless, following its implementation, platforms such as Meta, TikTok, and X introduced significant changes to their moderation policies. Meta implemented real-time content moderation reporting and external audits, while TikTok expanded fact-checking partnerships across Europe. These changes illustrate the impact of regulatory enforcement in compelling platforms to adopt responsible governance measures.

North America

Unlike the EU, the U.S. has historically prioritized platform self-regulation, justified by First Amendment protections which limits government intervention in speech regulation. Section 230 of the Communications Decency Act provides immunity to platforms for user-generated content while allowing them to moderate "in good faith," enabling them to moderate content without legal repercussions. However, debates over reforming Section 230 have intensified due to concerns about its role in enabling harmful content dissemination.

Case Study: U.S. Legislative Proposals

Legislative proposals such as the Platform Accountability and Transparency Act (PATA) advocate for greater algorithmic transparency, while the Protecting Americans from Dangerous Algorithms Act seeks to impose liability on platforms that amplify harmful content. Proposals such as the SAFE TECH Act aim to narrow its protections by holding platforms accountable for algorithmically amplified harmful content.

Stakeholders are deeply divided on this issue. Free speech advocates oppose reforms that could erode legal protections for lawful expression online. Civil society groups representing marginalized communities fear that increased liability pressures could incentivize platforms to over-moderate controversial but important speech. Meanwhile, industry stakeholders emphasize maintaining intermediary liability protections as essential for preserving innovation.

Latin America and the Caribbean

The LAC region presents a fragmented regulatory landscape for content governance and platform accountability, shaped by diverse political systems and socio-economic contexts. Brazil has emerged as a regional leader with its Marco Civil Law of the Internet and subsequent legislative proposals, setting a precedent for digital rights and platform regulation. Elsewhere in the region, Argentina's "Law on Intermediary Liability" establishes a notice-and-takedown system for copyright infringement claims.

Case Study: Brazil's Fake News Law

Brazil's Bill No. 2630, known as the "Fake News Law," seeks to combat misinformation by requiring platforms to store records of mass-forwarded messages for three months and banning external tools used for spam or misinformation dissemination. This law aims to enhance transparency in messaging services like WhatsApp, particularly during election periods. However, it has sparked debates on state overreach and platform responsibility. Platforms have expressed concerns about compliance costs associated with storing user data for extended periods and the potential impact on user privacy and freedom of expression. For instance, Brazil's Supreme Court suspended Telegram in 2022 for failing to comply with content moderation orders, highlighting the tension between government regulation and platform autonomy.

Asia-Pacific (APAC)

The APAC region exhibits a fragmented regulatory landscape due to varying levels of technological development and political priorities. Australia's Online Safety Act grants the eSafety Commissioner authority to demand the removal of harmful content within 24 hours, enforcing strict compliance on social media platforms. Conversely, the trio of China's Cybersecurity Law, Data Security Law, and Personal Information Protection Law mandate strict content censorship, prohibiting anti-government discourse and foreign digital influence.

Case Study: India's IT Rules

India's Intermediary Guidelines and Digital Media Ethics Code exemplify stringent regulations requiring platforms to appoint grievance officers and respond to takedown requests within 24 hours for flagged content related to national security or public order. It also requires platforms to trace and identify the originators of messages, compelling WhatsApp to challenge the law in court, arguing that it violates end-to-end encryption protections and user privacy rights. While proponents argue that these rules address critical issues like misinformation during elections by enhancing transparency in messaging services, critics highlight their potential misuse for political censorship. Civil society organizations have documented instances where government takedown requests targeted dissenting voices or critical journalism under vaguely defined terms such as "public order."

Stakeholder reactions reflect these tensions. Digital platforms operating in APAC express concerns about regulatory complexity across jurisdictions and high compliance costs associated with localized requirements, such us grievance officers or data localization mandates. Civil society groups warn that overly broad provisions could stifle freedom of expression and disproportionately affect marginalized communities.

Middle East and North Africa

In MENA countries, content governance policies frequently emphasize national security considerations and cultural preservation. Some governments in the region have implemented regulations that place limitations on certain forms of online expression, particularly content that could be perceived as inconsistent with national regulatory frameworks. Digital platforms operating in MENA nations encounter distinct challenges in navigating compliance with local legal frameworks while also aiming to protect user freedoms. The interplay between government regulations, platform policies, and individual rights in this region presents a complex landscape for content moderation and digital governance.

In 2022, the Saudi Communications, Space and Technology Commission (CST) and the General Authority for Media Regulation (Gmedia) requested that YouTube remove advertisements it deemed inconsistent with local cultural values and media regulations. The request was accompanied by a caution that non-compliance could result in legal action.

Many MENA countries have introduced cybercrime laws with broad provisions, which can be interpreted in ways that impact online discourse and content regulation. For example:

- Jordan implemented cybersecurity legislation that extends to cross-border content.
- The UAE has a Cybercrime Law that encompasses a wide range of online activities, including content that may conflict with official policies or geopolitical positions. Moreover, its Federal Decree-Law No. 55 of 2023 on Media Regulation establishes guidelines to guarantee that social media and gaming platforms assume full liability for anything posted on them. Media individuals and institutions operating in the UAE, including in the free zones, are required to comply with the national standards for media content.
- Kuwait amended its Penal Code in 2012, which imposes penalties on cases involving online expression such as blasphemy.

Case Study: Traditional vs modern media regulatory requirements

In Saudi Arabia, traditional media outlets operate under licensing requirements outlined in the draft Media Law, while digital platforms are not subject to the same licensing obligations but are expected to comply with content removal requests. This difference highlights the complexity of applying traditional regulatory models to modern digital platforms and invites ongoing reflection on how best to ensure coherence and consistency across media environments. However, the Kingdom has implemented advanced measures through its National Center of Information to counter misinformation while enhancing transparency in moderation practices. Additionally, CST launched its Digital Content Platform Regulations, a regulatory framework for digital content, which includes requirements for online audio and video streaming platforms as well as social media companies to comply with requests to remove content in line with the applicable law in the Kingdom. These positive initiatives include partnerships with social media companies to improve algorithmic fairness during crises such as elections or pandemics.

Sub-Saharan Africa (SSA)

SSA faces a range of challenges related to content governance and platform accountability. Limited digital infrastructure, inadequate regulatory frameworks, and political instability create obstacles to effective content moderation and governance. Many legal frameworks in the region were designed before the rise of digital platforms and are ill-equipped to address modern online harms, including election-related disinformation, hate speech targeting ethnic minorities, and digital surveillance abuses. Additionally, internet access and digital literacy remain unequal, exacerbating disparities in how content moderation policies affect different populations.

Nigeria, South Africa, and Ghana have taken steps toward strengthening content regulation. Nigeria's Digital Rights and Freedom Bill aims to protect users' online freedoms while regulating harmful content. The bill includes specific provisions for digital platforms, such as prohibiting them from being compelled to censor content without a court order and requiring them to protect legitimate expression. Additionally, platforms must implement complaint mechanisms to address online harm, particularly for protecting children. South Africa's Cybercrimes Act criminalizes the spread of harmful online content, including incitement to violence and cyber harassment. However, enforcement mechanisms remain weak, and concerns about government overreach persist.

Case Study: Content Moderation during Elections

Despite these challenges, several countries are making strides in content governance. Kenya's Election Monitoring Program provides a helpful case study. During Kenya's 2022 general elections, partnerships between social media platforms such as Meta and X resulted in significant reductions in false narratives circulating online. Platforms worked alongside fact-checking organizations, local election observers, and government agencies to curb misinformation. However, enforcement gaps remained, particularly in localized languages, which are often overlooked by globally standardized moderation algorithms. Misinformation in languages such as Swahili, Yoruba, and Hausa remains less frequently flagged compared to English or French, leading to inequitable moderation outcomes across linguistic groups.

DCO Landscape

Collectively, DCO's Member States have endorsed a Framework for Strengthening National Agendas to Combat Online Misinformation, adopted during the DCO's 4th General Assembly in February 2025, with the goal of guiding efforts to combat online misinformation.

Nationally, the landscape of content governance and platform accountability across Member States reflects a diverse regulatory approach, shaped by cultural, political, and technological contexts. Countries like Cyprus and Greece benefit from the comprehensive EU DSA, which introduces measures for platform transparency and accountability. In contrast, nations such as Djibouti and the Gambia operate under more general ICT laws that may not fully address platform accountability, particularly with regards to modern digital challenges. Middle Eastern members, including Kuwait, Oman, and Saudi Arabia, have implemented cybercrime laws that impact content moderation practices. Additionally, there is a growing trend towards data protection regulations, as seen in Bahrain's PDPL and Nigeria's NDPR, highlighting an increasing awareness of user privacy.

The table below provides a non-exhaustive list of the content governance and platform accountability policy landscape within the DCO ecosystem. It illustrates the varying levels of progress and maturity achieved by Member States and affirms the shared interest in ensuring that existing legislative frameworks are properly equipped to support the development of a responsible digital ecosystem.

Member State	Key Laws and Regulations	Relevance to Content Governance and Platform Accountability
Bahrain	PDPL (Law No. 30 of 2018)	Establishes data privacy obligations for online platforms, requiring transparency in data collection and content moderation decisions. Enhances user rights regarding personal data removal.
Bangladesh	Digital Security Act 2018	Grants authorities the power to remove or block content.
	Draft Data Protection Act	Aims to regulate platform accountability in handling user data and content governance, but concerns remain over government access to personal data.
Cyprus	EU Digital Services Act	Requires platforms to disclose content moderation policies, enhance algorithmic transparency, and implement due diligence to counter illegal content.
	National Cybersecurity Strategy	Strengthens platform accountability by setting security standards for digital content providers and requiring incident reporting for cyber threats.
Djibouti	Law n°66/AN/14/7ème L on Cybercrime	Criminalizes online misinformation, cyber fraud, and hate speech but lacks detailed provisions on platform liability and transparency.
The Gambia	Information and Communications Act 2009	Establishes content liability for ISPs, allowing for government oversight of digital platforms but lacks a clear appeals process for content takedowns.
Ghana	Cybersecurity Act 2020	Enhances platform accountability by introducing penalties for failure to regulate harmful content and requiring digital service providers to comply with safety measures.
	Data Protection Act 2012	Regulates data handling by online platforms, ensuring transparency and accountability in content governance decisions affecting user privacy.

Member State	Key Laws and Regulations	Relevance to Content Governance and Platform Accountability
Greece	EU Digital Services Act	Mandates systemic risk assessment for large platforms, algorithmic transparency, and user appeal mechanisms for content moderation.
	National Cybersecurity Strategy	Focuses on protecting critical digital infrastructure, indirectly impacting platform accountability in handling content-related cybersecurity risks.
Jordan	Cybercrime Law	Places restrictions on certain types of speech online, affecting platform responsibilities around content.
Kuwait	Law No. 63 of 2015 on Combating Cyber Crimes	Criminalizes online defamation, misinformation, and hacking, imposing liabilities on platforms for hosting illegal content.
Morocco	Law 09-08 on Protection of Personal Data	Ensures data privacy compliance for online platforms, requiring user consent and transparency in content moderation linked to personal data.
	Digital Development Agency	Promotes platform accountability and digital transformation through policy initiatives on content governance and misinformation control.
Nigeria	Nigeria Data Protection Regulation 2019	Requires platforms to protect user data, impacting content governance policies related to user-generated content and advertising.
	Cybercrimes Act 2015	Establishes platform liability for digital crimes, including fake news, cyberbullying, and online fraud, but enforcement remains inconsistent.
Oman	Cyber Crime Law	Criminalizes cyber threats and misuse of digital platforms, holding platforms accountable for content-related violations.
Pakistan	Prevention of Electronic Crimes Act 2016	Expands government authority over digital content, requiring platforms to remove "unlawful" content on demand.
	Personal Data Protection Bill (draft)	Aims to regulate platforms' data usage and ensure greater accountability in handling user content and personal information.
Qatar	Personal Data Privacy Protection Law No. 13 of 2016	Mandates platforms to safeguard user data, influencing content governance policies related to data-driven moderation.
	Cybercrime Prevention Law No. 14 of 2015	Establishes penalties for online offenses, enforcing platform responsibility in removing harmful or fraudulent content.
Rwanda	Law No 24.2016 on ICT	Provides a framework for digital governance, requiring platforms to comply with cybersecurity and content moderation standards.
	National Cyber Security Policy	Strengthens content governance oversight, particularly in preventing cybercrime and misinformation.
Saudi Arabia	Anti-Cyber Crime Law	Establishes strict regulations on digital content, requiring platforms to remove unlawful material and cooperate with authorities on content moderation policies.
	Draft Media Law (2023)	Defines the overarching rules and guidelines that govern media activities, including content moderation processes, and aims to provide clarity on content development and operating rules for media platforms.

4.4 Road Ahead

Europe

The EU and U.K. are likely to remain at the forefront of global efforts to regulate digital platforms, setting standards that may influence other regions. However, they must navigate tensions between safeguarding user rights and fostering innovation. The DSA's enforcement has led to debates about the balance between platform responsibilities and free speech. For instance, Amazon and Zalando have challenged their designation as VLOPs, arguing that their core business models differ from traditional content distribution platforms.

Latin America and the Caribbean

While the region has been slower to implement comprehensive digital regulations compared to Europe or North America, there is an increasing emphasis on developing policies that address misinformation, protect user data, and hold platforms accountable. The 2023 OECD/IDB Digital Government Index for LAC indicates progress in digital governance across the region, suggesting a growing capacity to address complex issues like content moderation. However, challenges remain in ensuring that regulations are adaptable to emerging technologies and do not inadvertently stifle innovation or infringe on digital rights.

Asia-Pacific (APAC)

Many countries are moving toward stronger rules for online platforms to remove harmful content. In some places, the government has strict control over what can be shared online, and platforms must follow strict rules. In contrast, countries like Japan and South Korea are trying to find a more balanced approach that holds platforms accountable while also protecting free speech. APAC is poised to become a leader in innovative approaches to content governance but must address challenges related to regulatory fragmentation and political interference. As such, we are likely to see increased adoption of mandatory reporting requirements for platforms in the region and cross-border collaboration on issues like misinformation during elections.

Middle East and North Africa (MENA)

MENA countries are likely to expand their focus on ethical AI use in moderation while addressing concerns related to freedom of expression. The integration of AI in content governance will expand, with the UAE's generative AI market projected to reach $2.036 billion by

Upcoming events

ACM FAccT Conference
Athens, Greece, 23-26 June, 2025

Find out more

Digital Marketing World Forum North America
New York, the U.S., 8-10 September, 2025

Find out more

Digital Marketing Europe
Amsterdam, Netherlands, 25-26 November, 2025

Find out more

2030, growing at 46.47%. This will enable more sophisticated, culturally sensitive content moderation, with AI tools analyzing regional dialects, cultural preferences, and local contexts to improve the accuracy and relevance of content filtering. Countries like Jordan and Egypt are implementing cross-border censorship laws targeting criticism of foreign governments, while the UAE enforces broad cybercrime statutes affecting platform operations. Efforts to support media accountability across 10 MENA countries, including promoting media literacy and decriminalizing defamation, will further impact how platforms are held accountable for the content they host and distribute.

Sub-Saharan Africa (SSA)

SSA has significant potential for growth in digital governance but requires sustained investment in infrastructure and capacity building. The region is still in the initial stages of developing comprehensive content governance frameworks, and many governments are exploring legislative reforms to address online harm. Regional bodies like the Economic Community of West African States (ECOWAS) have adopted strategies to bolster cybersecurity and combat cybercrime. Individual countries are also developing regulations to address online harm and enhance platform accountability.

5 Fair Competition

5.1 Overview

Fair competition in digital markets, particularly with regard to dominant digital platforms, is essential for sustainable economic growth and consumer protection. As certain platforms consolidate market share, robust and adaptive competition regulations are crucial to maintaining market openness. With roots tracing back to the Sherman Antitrust Act of 1890 in the U.S., fair competition is a well-established principle.

By 2020, over 125 jurisdictions worldwide had implemented competition law regimes, accompanied by active enforcement activities. As reflected in the design of many competition regulations, fair competition regulations aim to:

- Prevent monopolization by major players.
- Promote innovation and market entry for new players.
- Uphold consumer protection, including product safety, data privacy, fair pricing, and preventing deceptive practices.
- Ensure transparency to build trust, accountability, and prevent corruption.

These principles are vital for socio-economic sustainability, promoting innovation, enabling fair competition among digital platforms, and ensuring efficient resource allocation. They also enhance consumer welfare by ensuring access to high-quality products at reasonable prices and encouraging ethical practices.

The rapid expansion of the digital economy and the increasing influence of a few technology platforms have prompted policymakers to reconsider existing competition laws. Digital platforms have become some of the most influential economic actors globally, with several of the world's most valuable companies, such as Alphabet, Amazon, Apple, Meta, and Microsoft, centering their business models on digital services and ecosystems. This concentration has raised concerns among global policymakers about monopolistic practices and is motivating them to update their regulatory approaches.

The increasing influence of large global digital platforms presents unique challenges that traditional competition laws may not adequately address. These include:

- The difficulty in predicting future economic developments, leading to "winner-takes-all" scenarios.
- The prevalence of zero-price markets and self-preferencing practices.
- Algorithmic collusion, which can be hard to detect but results in higher prices.
- Specific challenges regarding merger controls due to vertical or conglomerate competition concerns.
- Expensive and time-consuming litigation against digital platforms, diverting resources from other areas.

Some policymakers have opted to leverage existing competition laws and issue additional guidelines for their application to dominant digital platforms, while others are developing new legislative frameworks and increasingly adopting an ex-ante approach. Ex-ante rules entail proactive measures that regulatory authorities implement to prevent potential issues before they arise, rather than being reactive. However, the transition to ex-ante legislation has faced pushbacks due to concerns about over-regulation stifling innovation, the need for a case-by-case approach, potential deterrent effects on foreign investment, and increased compliance costs.

The future of digital platform competition regulation requires a balanced approach, fostering international cooperation among regulators, industry stakeholders, and policymakers. Fair competition rules are increasingly expected to adapt to technological advancements and evolving digital market dynamics, aiming to promote transparency and accountability in how platforms operate across global markets.

5.2 Latest Developments

The fair competition landscape has seen significant developments over the last couple of years:

Policy Developments

The EU's DMA came into force in March 2024 to regulate large online platforms designated as "gatekeepers," and in the same year, concluded that the social networking service X does not qualify as a core platform service, exempting it from certain obligations, such as self-preferencing rules.

The U.K. Digital Markets, Competition, and Consumers Act (DMCC) received Royal Assent in May 2024. It introduces new powers for the Competition and Markets Authority (CMA), including the designation of Strategic Market Status (SMS) for firms with substantial entrenched market power. The Act aims to ensure fair competition by enforcing conduct requirements on designated firms and facilitating pro-competitive interventions.

Amendments to the Canadian Competition Act brought significant changes to the merger review process, including changing certain statutory market concentration thresholds that would prevent or lessen competition. This enhances the Competition Bureau's ability to scrutinize acquisitions by dominant platforms.

Brazil's Ministry of Finance launched a public consultation in 2024 focused on the economic and competitive aspects of digital platforms. The aim was to assess the need for changes to the country's competition law, including the creation of a specific regulatory body, defining and categorizing digital platforms, and determining specific aspects related to digital markets that may be subject to additional regulation.

In 2024, the national competition authorities of South Africa and Angola signed a Memorandum of Understanding (MoU) to increase their cooperation in the field of competition law.

In late 2024, amendments to the Turkish Competition Act were in their final legislative stages, intended to support the regulation of digital markets through enhanced powers to investigate algorithmic pricing and platform neutrality.

The Australian Competition and Consumer Commission launched a public consultation in 2024 on its new digital competition regime. The proposal included potential ex-ante rules for dominant platforms.

Global Initiatives

- In 2024, the OECD published a report entitled "Competition Policy in Digital Markets: The Combined Effect of Ex Ante and Ex Post Instruments in G7 Jurisdictions," identifying key competition concerns, compliance strategies and exploring the global implications of national enforcement activities.

- In March 2024, the International Competition Network (ICN) held its first Technologist Forum, focused on strengthening and supporting law enforcement agencies navigating digital markets.

- The UNCTAD Intergovernmental Group of Experts on Competition Law held a session in July 2024, focused on policy challenges in the digital market, and best practices to balance innovation and sustainable growth alongside the prevention of anti-competitive conduct.

5.3 Regional Approaches

Europe

Europe has developed a comprehensive competition framework for digital markets. The EU's DMA, adopted in 2022 and enforced from March 2024, is one of the most significant global regulatory efforts targeting competition in the digital economy. It aims to address structural imbalances between large online platforms and smaller market participants by establishing a set of ex-ante obligations for designated "gatekeepers."

Features of the DMA

To qualify as a gatekeeper, a platform must have an annual turnover of at least EUR 7.5 billion $8 billion) in the EU or a market valuation of EUR 75 billion ($81 billion) and must provide a core platform service with at least 45 million monthly active end-users and 10,000 annual business users within the EU. Gatekeepers are subject to a series of obligations, including prohibitions on self-preferencing, requirements to allow third-party interoperability, restrictions on combining personal data across services without user consent, and mandates to enable users to uninstall pre-installed apps. Non-compliance can result in fines of up to 10% of a company's total worldwide turnover, rising to 20% for repeated violations. In cases of systematic non-compliance, the European Commission may impose additional remedies, including structural measures such as divestitures.

These Gatekeepers, including Alphabet, ByteDance, Meta, Microsoft, Amazon, and Apple, face specific obligations to prevent market abuse and ensure consumer choice. Changes include Apple allowing alternative app stores, Meta making WhatsApp interoperable, and Google giving EU users more data control.

The financial impact of the DMA remains debated. The European Commission estimates an annual consumer benefit of $14 million, while others foresee potential compliance costs for U.S. providers of up to $50 billion in, equivalent to 17% of their EU revenues. SMEs report rising operational costs and competitive concerns. While some view this as a necessary shift toward market fairness, others warn of burdens on innovation and investment.

The U.K.'s Digital Markets, Competition and Consumers Act (DMCC), effective April 2025, establishes a new regulatory unit and designates companies with Strategic Market Status (SMS) – defined by annual U.K. revenues of over GBP 1 billion ($1 billion) or global revenues of GBP 25 billion ($31 billion), alongside entrenched and substantial market power. Similar to the EU's gatekeepers, SMS firms face stringent regulations. The U.K. government predicts $1 billion annual consumer benefit, but some caution that increased costs could reduce digital investment.

Case Study: Google-Android in the EU

In September 2022, the General Court of the EU upheld the European Commission's 2018 decision that found Google had abused its dominant position in the market for Android mobile devices. The case centered on Google's requirement for manufacturers to pre-install Google Search and Chrome as a condition to access the Google Play Store, as well as restrictions on using alternative versions of Android. The court confirmed this violated EU competition law under Article 102 of the Treaty on the Functioning of the EU and imposed a fine of EUR 4.125 billion ($4.5 billion). This decision contributes to the broader enforcement of digital antitrust in Europe and supports the DMA.

North America

The North American competition landscape is shaped by a combination of regulatory frameworks, enforcement actions, and legislative initiatives. In Canada, two key developments stand out. First, the Canadian Digital Regulators Forum was established in 2023, bringing together the Competition Bureau, the Radio-television and Telecommunications Commission, the Office of the Privacy Commissioner, and the Copyright Board to collaborate on digital market and platform issues. Second, Canada updated its Competition Act in 2022 and 2023, clarifying criteria for determining market dominance. This is particularly relevant for digital markets, where large technology companies must comply with additional regulations due to their market dominance.

In the U.S., the Federal Trade Commission (FTC) and the Department of Justice (DOJ) enforce federal antitrust laws through the Sherman Act, the Clayton Act, and the Federal Trade Commission Act. However, there is no digital-specific legislation. The American Innovation and Choice Online Act and the Open App Markets Act were voted out of committee in early 2022 but are unlikely to pass. Federal legislation is supported by state-level actions, such as State Antitrust laws and Unfair Trade Practices, with agencies in New York and California working closely with the FTC and DOJ.

Case Study: Antitrust Enforcement in the U.S.

In 2023-2024, the U.S. saw a wave of antitrust proceedings against major digital platforms, marking one of the most significant government-led challenges to platform dominance in over a decade. In 2023, the FTC and 17 state attorneys general sued Amazon for anticompetitive practices. Allegations included stifling competition, inflating prices, and degrading quality. In 2024, Amazon won a partial dismissal, with some claims proceeding and others dismissed. The case will be tried in two parts, addressing alleged violations and proposed remedies separately.

In a parallel development, the DOJ filed a case seeking to break up Google's advertising business, citing antitrust violations and arguing the company maintained monopolies in search advertising markets.

As the Trump administration continues into 2025, the regulatory direction remains uncertain. Some observers anticipate a rollback of enforcement intensity, while others note that bipartisan scrutiny of large tech platforms may sustain legal momentum. These proceedings underscore the growing complexity of regulating platform power in the U.S., where litigation-based approaches remain the primary tool in the absence of new federal digital competition legislation.

Latin America and the Caribbean

In the LAC region, Brazil is a key advocate for ex-ante, digital-specific competition rules. In 2021, Brazil introduced guidelines on how existing competition regulations apply to digital platforms. In November 2022, Bill No. 2768/2022 was introduced, inspired by the EU's DMA. This bill, still under discussion in early 2025, aims to establish an ex-ante regulatory regime for digital platforms, with the National Telecommunications Agency (ANATEL) and the Administrative Council for Economic Defense (CADE) as key authorities. The Latin American Internet Association (ALAI) has raised concerns about the bill's economic impact and the vulnerability of SMEs.

In Mexico, the Federal Economic Competition Commission (COFECE) established a Digital Markets Competition Unit in 2020 as part of a broader digital strategy. Since President Claudia Sheinbaum's election in 2024, the focus has shifted to increasing connectivity, accessibility to digital services, and digitizing government services, rather than promoting competition. This trend is seen across the region. Between 2015 and 2020, competition authorities in Argentina, Colombia, and Chile investigated anticompetitive conduct, focusing on mergers.

Experts note that LAC governments prioritize digital infrastructure development, education, and service quality over competition issues. In 2022, there were 893 online marketplaces in the region, with Amazon often losing out to local competitors like Mercado Libre. Consequently, competition in digital markets is less of a priority for LAC governments.

Case Study: Mercado Libre in Brazil

Mercado Libre was found guilty of unfair competition by the 1st Business Court of São Paulo for using the keyword "Verisure" in Google ads to direct consumers away from the security company's site. The court determined that this practice violated Verisure's exclusive brand usage rights. Mercado Libre contended that it did not engage in the same business activity as Verisure, but the court upheld the ruling. The decision included monetary and moral damages, with the exact amount to be determined later.

Asia-Pacific (APAC)

Across the APAC region, there is no clear consensus on the best approach to digital competition regulation. Some countries have updated existing regulations with additional legislation or flexible guidelines, while others are considering an EU-inspired ex-ante approach. The Taiwan Fair-Trade Commission has expressed skepticism towards the EU's DMA and the shift away from ex-post controls.

India's Digital Competition Bill and Australia's new proposed digital competition regime, are closely aligned with the EU DMA. Indonesia is considering using the EU DMA as a reference for its own platform governance, with businesses viewing it as a "navigation tool" for the Indonesian digital market. Singapore's Competition and Consumer Protection Commission (CCCS) has opted for public consultations and issued guidelines on digital competition.

Japan and South Korea are pursuing a dual approach, combining ex-ante legislation with new frameworks and guidelines for the digital market. Japan's Digital Platform Guidelines 2020 provide

clarity on various digital economy issues, while the Act on the Promotion of Competition in Relation to Specified Software Used in Smartphones is similar to the EU DMA but narrower in scope. South Korea's Guidelines for Review of Abuse of Market Dominance by Online Platform Operators took effect in January 2023, and the New Digital Competition Bill has raised concerns about favoring Chinese technology companies. This reflects the broader regional debate on adapting EU DMA principles to local contexts. For its part, China has taken a unique path in digital competition enforcement, characterized by a series of regulatory interventions targeting some of its largest domestic platforms. Since 2020, the government has imposed penalties and restrictions on companies like Alibaba, Meituan, and Tencent, citing concerns over consumer rights, data privacy, and market abuses. For example, Alibaba was fined $2.8 billion in 2021 for abusing its dominant position in e-commerce. However, signs of a policy recalibration emerged in late 2024, with President Xi Jinping meeting leading tech CEOs, signaling a potential softening of regulatory posture aimed at revitalizing private sector confidence and investment.

Case Study: Alphabet in India

The Competition Commission of India (CCI) opened an investigation into Google in November 2024, ordering a detailed investigation into the company in connection with a complaint filed by Winzo Games for alleged unfair business practices with respect to the listing of real money gaming apps on the Play Store. This initiative signifies a step towards fostering fair competition in India's digital ecosystem. It is set to examine Google's business practices and their potential impact on the competitive landscape. The investigation stands out as a significant development in India's efforts to regulate digital markets and ensure a level playing field for businesses.

Middle East and North Africa (MENA)

In the MENA region, fair competition in digital markets has received less attention compared to other regions. While digital infrastructure development and economic diversification are high priorities, digital-specific competition laws are still emerging. Several jurisdictions continue to rely on general competition laws, which may not fully address the market dynamics of digital platforms. In countries like Lebanon, Jordan, Oman, and Iraq, enforcement of general competition regulations is low, and few have introduced platform-specific rules to address concerns such as data concentration, algorithmic transparency, or market access barriers.

However, Gulf countries are updating their competition laws. Saudi Arabia is revising its Media Law to protect digital users, including guidelines for content removal and moderation and enhanced cybersecurity. This is part of ongoing efforts to develop competition regulations since 2019. The UAE updated its competition laws at the end of 2023, and Qatar's Communications Regulatory Authority is creating measures to monitor and respond to market power and competition, including regulations for digital services and data use.

Sub-Saharan Africa (SSA)

Since 2020, the Competition Commission of South Africa (CCSA) has focused on the unique challenges digital markets pose to fair competition regulations. It has updated its approach to detect and prevent collusion, address market dominance abuse, and increase control over mergers and acquisitions. In 2023, after an Online Intermediation Platforms Market Enquiry, the CCSA chose to leverage existing regulations and tools rather than create a new framework. It recognized the reduction of national media plurality due to practices by Meta,

Google, OpenAI, TikTok, and others, and urged Google to stop its "search bias in favor of foreign media."

Beyond South Africa, it is increasingly common for one authority to enforce both competition and consumer protection mandates, as seen in Nigeria, Kenya, Zambia, and Malawi. For instance, Nigeria has supplemented its competition law with a Notice on Market Definition, adopting a flexible soft-law approach.

Two notable initiatives in Sub-Saharan Africa extend beyond national borders: the Africa Heads of Competition Authorities Dialogue (AHCAD), a regional network promoting best practices and collaboration, and the Common Market for Eastern and Southern Africa (COMESA), which supports national competition authorities in implementing privacy, consumer protection, and other laws, driving capacity-building initiatives.

Case Study: Meta in South Africa

GovChat, a South African civic engagement platform, won its legal battle against Meta but faced significant financial and resource burdens. The dispute involved Meta's attempt to remove GovChat from its WhatsApp Business platform, essential for GovChat's communication with South African citizens. Although GovChat maintained access, the lengthy legal process was costly, highlighting the challenges smaller entities face against large tech corporations. This case underscores the power imbalance and the importance of access to communication platforms for civic engagement and government service delivery.

DCO Landscape

Fair competition is integral to the DCO policy objectives and its application to digital markets is being explored across all DCO Member States. As part of the DCO Roadmap, Goal 3 focuses on creating a responsible digital ecosystem, and as earlier established, fair competition is vital to this ambition.

The table below provides a non-exhaustive list of the fair competition policy landscape within the DCO ecosystem, as it relates to digital markets. It illustrates the varying levels of progress and maturity achieved by Member States and affirms the shared interest in ensuring that existing legislative frameworks are properly equipped to ensure fair competition in digital markets.

Member State	Key Laws and Regulation	Relevance to Digital Markets
Bahrain	Law. No. 31	Bahrain updated its Competition Promotion and Protection Law in 2018, including new rules to target anti-competitive practices in digital markets.
Bangladesh	Competition Act 2012	In addition to its Competition Law, Bangladesh has announced that it is drafting new policies to enhance its digital governance framework.
Cyprus	Protection of Competition Law 2022	A 2024 amendment to the Competition Law sought to align Cyprus' national competition regulation with the EU's DMA.
Djibouti	Law on Competition, Fraud Repression and Consumer Protection (No. 2011-030)	Djibouti's Competition Law includes provisions that serve to combat anti-competitive practices in digital markets. Djibouti is also part of COMESA and is engaging in discussions to ensure that competition regulations address digital market challenges.
Gambia	Competition Act, No. 4 of 2007	In addition to its primary competition legislation, the Gambian national competition authority has initiated market studies to better understand the dynamics of the digital market. The Gambia is a member of ECOWAS Regional Competition Authority and one of the focus areas is digital market regulations and enforcements.
Ghana	Protection Against Unfair Competition Act, 2001 (Act 589) Consumer Protection Act 2012	The Competition Act and Consumer Protection Act apply to digital markets and Ghana is also conducting market studies to identify areas for regulatory improvement in digital market. Ghana is a member of the ECOWAS Regional Competition Authority and is aligning its competition laws with the African Continental Free Trade Area (AfCFTA) framework to enhance cross-border digital market transactions.
Greece	Act No. 5099/2024 (2024)	Greece transposed the EU Digital Markets Act into Greek Law in 2024.
Jordan	Competition Law in 2004 (No. 33/2004),	Jordan's Competition Law is undergoing parliamentary review in early 2025 and its impact on digital markets is as yet unconfirmed.
Kuwait	Protection of Competition Law (Law No. 72 of 2020)	Kuwait's Competition Law includes provisions that serve to combat anti-competitive practices in digital markets.

Member State	Key Laws and Regulation	Relevance to Digital Markets
Morocco	Competition Law No. 12.104 (2014) and 40.21 (2022) & Guidelines for Digital Markets	To bolster its Competition Law, Morocco has issued guidelines clarifying its application to digital markets. In 2023, the Competition Council updated the merger control regime.
Nigeria	Federal Competition and Consumer Protection Bill 2018 (FCCPA)	Nigeria's Competition Law includes provisions that serve to combat anti-competitive practices in digital markets and the FCCPA introduced new merger control regulations in 2021.
Oman	Oman Competition Protection and Monopoly Prevention Law (Royal Decree No. 67/2014, as amended by Royal Decree No. 22/2018) & Executive Regulations (2021)	Executive Regulations issued in 2021 clarify the application of the Competition Law to digital markets, addressing issues such as market dominance.
Pakistan	Competition Act 2010	In addition to existing legislation, the Competition Commission of Pakistan (CCP) launched a study of digital markets in 2024, intended to inform the proposal of a Digital Market Competition Bill.
Qatar	Law No.19 of 2006 on the Protection of Competition and the Prevention of Monopolistic Practices, Competition Policy 2015	The Communications Regulatory Authority (CRA) is conducting a review of national competition law and is expected to provide specific regulations on the operation of digital platforms.
Rwanda	Law on Competition and Consumer Protection (2012) Competition and Consumer Protection Policy 2023 (CCP)	Competition Law is strengthened by the 2023 revision of the Competition and Consumer Policy, which addresses challenges posed by the digital economy.
Saudi Arabia	Competition Law (2019) Competition Regulations for Digital Content Platforms 2022 Media Law, covering Digital Service Providers (under review)	The Kingdom issued specific regulations for digital content platforms in 2022, having issued more general competition laws in 2019. The ongoing strategic review of the Media Law is expected to include several measures to protect users of digital platforms.

5.4 Road Ahead

The landscape of digital platform competition regulations is poised for significant evolution in the coming years, with policymakers weighing the need for stronger enforcement against the risks of over-regulation stifling innovation or deterring foreign investment. The geopolitical dimension of these regulatory shifts is increasingly relevant as concerns that the EU's DMA disproportionately affects U.S. technology firms have prompted scrutiny from U.S. policymakers and are influencing ongoing debates about transatlantic digital trade relations.

The European Commission's ambition for the "Brussels Effect", where EU regulations shape global competition policies, is gaining traction in the U.K., Australia, Brazil, and India, driven by concerns that existing frameworks do not adequately address platform dominance and anti-competitive behavior. However, Latin America and parts of APAC remain divided on the necessity of ex-ante regulation, with some nations favoring case-by-case enforcement under existing antitrust laws. While the EU and U.K. project long-term economic benefits from their new regulatory frameworks, critics argue that compliance costs and regulatory uncertainty could impact market growth.

Moving forward, competition regulations for digital platforms must remain adaptable, allowing authorities to address emerging platform dominance issues while keeping pace with rapid technological advancements. International collaboration will be crucial for aligning regulatory approaches, ensuring that digital platforms adhere to high competition standards across jurisdictions, and fostering a fair, innovation-driven digital economy that prioritizes consumer welfare and market openness.

Upcoming events

34th Annual IBA Communications and Competition Law Conference
April 28-29, 2025, Paris, France

Find out more

International Competition Network (ICN) Annual Conference
May 6-9, 2025, Edinburgh, U.K.

Find out more

OECD Global Forum on Competition
December 2025, Paris, France

Find out more

Document Disclaimer

The following legal disclaimer ("Disclaimer") applies to this document ("Document") and by accessing or using the Document, you ("User" or "Reader") acknowledge and agree to be bound by this Disclaimer. If you do not agree to this Disclaimer, please refrain from using the Document.

This Document, prepared by the Digital Cooperation Organization (DCO). While reasonable efforts have been made to ensure accuracy and relevance of the information provided, the DCO makes no representation or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability or availability of the information contained in this Document.

The information provided in this Document is intended for general informational purposes only and should not be considered as professional advice. The DCO disclaims any liability for any actions taken or not taken based on the information provided in this Document.

The DCO reserves the right to update, modify or remove content from this Document without prior notice. The publication of this Document does not create a consultant-client relationship between the DCO and the User.

The designations employed in this Document of the material on any map do not imply the expression of any opinion whatsoever on the part of the DCO concerning the legal status of any country, territory, city, or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

The use of this Document is solely at the User's own risk. Under no circumstances shall the DCO be liable for any loss, damage, including but not limited to, direct or indirect or consequential loss or damage, or any loss whatsoever arising from the use of this Document.

Unless expressly stated otherwise, the findings, interpretations and conclusions expressed in this Document do not necessarily represent the views of the DCO. The User shall not reproduce any content of this Document without obtaining the DCO's consent or shall provide a reference to the DCO's information in all cases.

By accessing and using this Document, the Reader acknowledges and agrees to the terms of this Disclaimer, which is subject to change without notice, and any updates will be effective upon posting.

Digital Cooperation Organization

Follow us on

@dcorg

www.dco.org