ARTICLE

The Era of Digital Regulation

How content is created and shared on digital platforms is coming under increasing scrutiny with Regulators and the public calling for online platforms to take on more responsibility. Regulation has been on the horizon with France coming close to passing law to regulate online hate speech (subsequently struck down in court due to freedom of speech concerns) and the Online Harms Bill was proposed by the UK in 2019.

More recently, the European Commission (EC) published its proposal for the Digital Services Act (DSA), which intends to update the horizontal regulatory framework for digital services. This represents an ambitious attempt at updating the rules that govern the digital sphere and will introduce due diligence obligations for online intermediaries in addition to safeguards, transparency measures and new enforcement powers for authorities.

The European Union has also proposed a Digital Markets Act to harmonise measures to encourage fair and open digital markets.

The passage and enactment of these regulations may take years, and the text will likely change in deliberations. However, given the groundswell of scrutiny, digital platforms and companies operating in this space should consider taking proactive steps towards establishing digital trust and tackling the challenges that lay ahead.

What Does this Mean for Digital Services Providers?

— **New Responsibilities** – Digital Service Providers (DSPs) under the DSA could have a wide variety of new obligations depending on their designation under the Act. Very large platforms and Online platforms will be expected to appoint contact points and legal representatives, adopt reporting obligations, set terms and conditions, introduce new processes and protocols, among other responsibilities. The Online Harms Bill proposes similar requirements, including a code of conduct that sets out responsibilities towards children and introduces a code of conduct. The Bill will also place a responsibility on DSPs to combat misinformation, with Ofcom having enforcement power.

— **Fines** – The Online Harms Bill will no longer seek to introduce criminal liability for executives for non-compliance. However, it does provide Ofcom with the ability to fine non-compliant organisations with fines of £18 million or 10% of global turnover. Similarly, the DSA introduces enforcement actions, including fines of up to 6% turnover in the previous year, inspections

and periodic penalty payments. The DMA will enable sanctions of up to 10% of worldwide turnover for non-compliant gatekeepers.

What should DSPs start doing now?

— **Establish Governance and Reporting** – a multi-disciplinary team should be established to help manage content and act as a decision-making body. Once a multi-disciplinary team has been established, reporting lines should be documented with clear externally-facing contact points. The reporting lines should be directed to the executive level to ensure that events are addressed swiftly. There will be significant operational challenges posed by the regulations' implementation, and effective governance will help streamline some of these challenges.

— **Identify Solutions and Design Workflows to Reduce Burden and Time** – DSPs should consider adopting predictive approaches to blocking content using keyword and content coding, and by leveraging analytics and machine learning to flag and block content at speed. Hate speech detection technology can be tricky to implement in practice, due to the lack of consensus of clear definitions of hate speech, wherein context is critical. Depending on the platform, typos or coded language may result in false negatives. Time should be invested in defining a robust workflow to help DSPs in the ongoing battle against harmful content. Solutions are only as good as their design, and it is important that predictive analytics and machine learning are configured to fit the business's needs. Effective technology can help combat the speed and scale of dissemination of content and reduce the lead time to remove harmful content.

— **Understand the Data You Hold** – DSPs should proactively map out data transfers, identify data flows to review sharing practices and understand how content is shared with third parties. In recent months, several businesses have suffered damage to their brand due to their sharing practices.

— **Know Your Trader** – Online marketplaces will need to ensure the traceability of goods, including identifying illegal goods. Firms may consider leveraging KYC automation tools to automate identity verification and product authentication technology.

— **Build Transparency** – Trust is at the heart of these regulations and is quickly becoming a competitive differentiator. Establish trust with users by communicating what is being done to meet digital compliance obligations and what online safeguards are in place. If algorithms are used, DSPs should explain how these are used and their impacts on accessible consumer-facing policies and reflected in codes of conduct.

— **Data Minimisation and Retention** – It will be important to clearly define how long content is available and what retention periods should apply, especially for personal data. A global retention schedule will reflect business, regulatory and legal requirements and enable business decisions regarding how long data is retained and where it is stored. Disposing of data that has no value to your organisation will enable compliance with data minimisation principles and reduce risk and cost.

— **Conduct Independent Audit** – Commence engaging independent external experts to assess compliance with the legislation and develop approaches to audit algorithmic systems effectively.

One of the driving motivations behind these regulations is to generate transparency and trust in the digital sphere. As a first measure, DSPs should take steps to facilitate transparency and trust. Demonstrating to consumers how they are meeting their digital obligations will also provide a clear signal to regulators—and their customers—that compliance and transparency are priorities.

The views expressed in this article are those of the author(s) and not necessarily the views of FTI Consulting, its management, its subsidiaries, its affiliates, or its other professionals.

RAJIV RADHAKRISHNAN
+44 (0) 781 428 0318
rajiv.radhakrishnan@fticonsulting.com

JACK FLETCHER
+44 (0) 7779431010
jack.fletcher@fticonsulting.com

1312 - 02/21