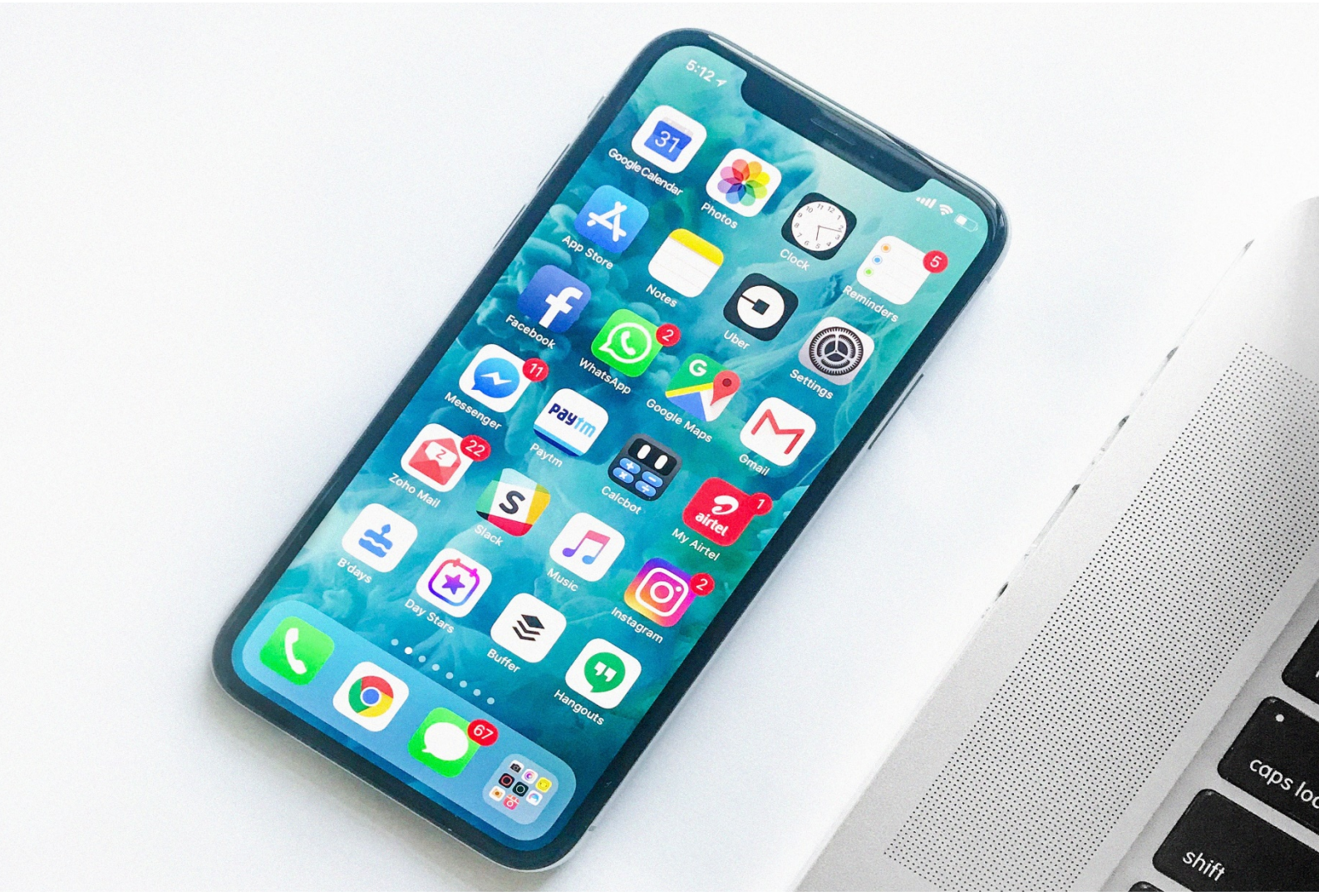

Free Speech vs Fake News: The Future of Content Regulation

Anne Shannon Baxter, Policy Manager, Multilateral Organisations
Tiernan Kenny, Policy Manager, UK&Europe
Logan Finucan, Senior Manager, Data Policy & Trust
Seha Yatim, Policy Manager, Asia & US

Advances in technology over the past decade, combined with the current intermediary liability regime – created under the e-Commerce Directive in Europe and § 230 of the Communications Decency Act in the US ("Section 230") – has led to the massive success of digital platforms and the booming development of the online space as we know it today. Indeed, the combination of these two factors has cemented the role of digital platforms as increasingly influential – and powerful – actors in modern economies and societies across the globe.

For many, however, this has brought heightened challenges that risk impacting citizens worldwide. From a users' lack of control over their personal data to the potential of exposure to online harms; from disinformation to the threat of undue exposure to foreign influence; from inadequate treatment of platform workers; to competition and taxation.

Trust is fundamental to the working of the digital economy. However, the way these challenges have been dealt with and the anti-tech narrative which has developed, have eroded many stakeholders' trust in technology companies and technology itself. There is a growing notion that technology companies cannot

– or will not – act unilaterally to resolve these issues and that government intervention is required to level the playing field.

In recent years, policymakers have been reconsidering intermediary liability regimes, placing increased pressure on technology companies to control the content on their platforms. In many instances the rules that apply to platforms are outdated. We need to revise the rules in a way that protects users and fosters trust but also continues to facilitate the growth and development of the digital economy that has brought so many benefits and has the potential to deliver more.

Where Are We Heading?

Many non-US policymakers are resentful that the world's leading platforms are operated by American companies – and that they have integrated American values into their operations and spread these values as they have expanded globally. Policymakers across the globe are developing new frameworks that will guide technology development, in line with their respective principles to serve their citizens.

EU Digital Services Act: Content Regulated

The European Commission is preparing for a big push on content regulation, as part of its overall move towards 'digital sovereignty'. Emboldened by the global impact of the General Data Protection Regulation ("GDPR"), coupled with a low-held desire to address the dominance of both American and Chinese technology companies, policymakers in Brussels are preparing the so-called "Digital Services Act" (DSA), a wide-ranging legislative package in an attempt to regulate the online world.

The DSA will include a revision of the e-Commerce Directive ("ECD"). The ECD, broadly analogous to Section 230, provides wide-ranging intermediary liability protections relied upon not just by platforms, but almost every business operating online to avoid liability for content they host, cache or transmit. Changes to these long-established rules could have a significant impact on the internet ecosystem by making internet companies liable for the harm caused by illegal or harmful content shared through their platforms or services. At the time of writing, it appears unlikely that the European Commission will propose entirely removing the broad liability protections or the prohibition on general monitoring, however, there is a clear political call for online platforms to take more responsibility for the content they host online.

The enormous growth of some online platforms and the systemic role they play in daily life across the EU has convinced the European Commission that the current framework, dating from 2000, needs to be updated and that platforms need to take more responsibility for their involvement in the internet ecosystem. Following similar debates on Section 230 in the United States and recent court decisions in India, EU policymakers want to act fast and set the de-facto global content regulation standards in the same way as they did with GDPR. The European Commission is also wary of initiatives such as France's draft 'hate speech law' and the UK's progress on online harms. There is a fear that different national approaches to content regulation will damage the EU's Digital Single Market, and the pan-EU harmonisation it intends to create. A further example of an EU member states' unilateral action is Germany's recent update to its NetzDG law to introduce proactive obligations for social media companies to seek out and remove certain types of hate speech.

While the European Commission may try to adopt a narrow focus, giving platforms new obligations to tackle illegal content, some members of the European Parliament will try to expand the scope of any new rules. This could include duties of care, obligations to pro-actively remove harmful or distasteful content or force larger platforms to develop and share content moderation tools with competitors. Member states may also push for strict rules on fake news and disinformation, fearful of electoral interference, or even

attempts to manipulate stock markets with deep-fake videos of business leaders. The challenge for policymakers is to succinctly define the problem they are trying to solve and create a regulatory regime which does not incentivise platforms to censor their platforms.

Preparations for the DSA are well underway and legislative proposals are expected towards the end of 2020.

United States:

In the US, too, regulation of platforms and online content may be shifting in response to both law enforcement pressure and politically charged concerns over online speech. The basis for the regulation of platforms and services only has been relatively stable since 1996 when the Communications Decency Act was adopted. Section 230 of that Act provides broad, immunity for online platforms with which users interact – this immunity is two-fold: 1) they are not liable as the speaker of content placed there by users; and 2) they are not liable for loss or harm resulting from efforts of good faith to remove illegal or objectionable content. While most often associated with user-content focused services like social networking sites, these protections apply to a broad range of online businesses, from web-hosting and content delivery networks, to home-sharing and e-commerce.

However, this foundation for the online economy has come under increasing pressure in recent years, for various reasons. In 2018, Congress enacted the most dramatic erosion of Section 230 protections to date with the joint *Stop Enabling Sex Traffickers Act* and *Allow States and Victims to Fight Online Sex Trafficking Act*. While these joint acts did not change the fundamental characteristics of Section 230, they carved out a wide space for enforcement to target sex trafficking through online platforms. The measures have created a criminal offence that may be committed by parties to a venture that promotes or facilitates prostitution (18 USC 1591), and specifically denies the protections of Section 230 with regard to enforcement of the newly-created criminal statute.

The challenges to Section 230 are far from over, however, and there are calls for further changes, especially regarding social media. Law enforcement still feel that protected platforms are insufficiently responsive to their requests, or wilfully ignore types of illegal content, especially with regards to sex trafficking and sexual exploitation of children. Additionally, the issues of online political speech, misinformation, and radicalisation have politicised these protections, giving rise to two power – and in fact contradictory – motivations fuelling calls to re-consider the protections afforded by Section 230. Conservatives feel that protected platforms are abusing their immunity regarding content removal to stifle political speech. In contrast, Democrats and liberals feel that these platforms are not doing enough to remove objectively false and harmful speech.

Several proposals are currently circulating in Congress which could alter Section 230, some by stripping protections for those which moderate or filter political speech in a politically biased manner, others by barring algorithmic personalisation of content altogether. A further proposal conditions enjoyment of protections on unrelated issues such as use of encryption in digital communications.

While the COVID-19 crisis has temporarily stalled most legislative efforts and may offer technology companies some respite from 'techlash,' it may not bury concern over Section 230, particularly in terms of social media. Facebook's efforts to remove COVID-19 related misinformation and calls to violate social distancing norms have already rankled both those who say they are not doing enough and those who say they are going too far.

India

India is set to revise existing guidelines to regulate internet intermediaries. The guidelines aim to hold companies liable for the content that is hosted and shared on their online platforms. Aside from making content filters mandatory, the guidelines require companies to be able to trace all content and metadata back to users, take down offensive content within 24 hours and have local offices in India. The government has also introduced a data protection law, which closely emulates GDPR. However, new rules state that companies must hand over non-personal data of their users to the government.

These two regulations, along with vague definitions of some important terms, pose major compliance issues for technology platforms. The regulations shift the burden of defining and removing what is 'illegal' content back to platforms and raise legitimate concerns regarding state overreach and self-censorship.

Singapore

Last year, Singapore passed a fake news law providing the government with the power to stop the spread of fake news on any platform. The government passed the Protection from Online Falsehoods and Manipulation Act (POFMA) in May 2019, which came into force in October 2019. The POFMA has a broad scope and raises concerns with regards to its implementation. It mandates users and/or platforms to take down offending content and requires them to display a correction notice.

Singapore prefers to use the term 'falsehoods' meaning the deliberate spread of false information or news. The law is an effort towards content regulation on social media platforms. Existing laws like the Telecommunications Act and the Broadcasting Act also criminalise falsehoods.

Self-Regulation – Is There Still Space for It?

Historically, technology companies have made varied attempts to self-regulate to stave off government censorship and protect free speech. This is ultimately an economic motivation – platforms need to create environments that will drive user engagement and lead users to choose their platform over others. A study published by the Harvard Law Review identified three main reasons why leading American platforms (Twitter, Facebook and YouTube) engage in moderation: 1) an underlying belief in free speech norms; 2) a sense of corporate responsibility; and 3) the necessity of meeting users' norms for economic viability. As platforms expand and gain an unprecedented number of users, self-regulation has become increasingly difficult to manage. Governments are increasingly holding technology companies responsible for the content on their platforms. The technology industry needs to act as one and work closely with governments to ensure the development of smart and fair regulations.

What We Need to Do Now

It is critical to educate stakeholders on the technology ecosystem and the impact of updated content regulation rules to avoid your businesses being hit with poorly drafted rules and increased liability. Content regulation legislation is often drafted with a limited number of internet companies in mind, without consideration of the unintended effects on smaller players or companies in different parts of the internet value chain. All companies have work to do to ensure that policymakers have a clear view of the modern digital economy and how the different cogs interact to turn the wheel of economic growth.

This can be achieved through the formation of coalitions of like-minded operators, which can offer a coherent industry voice, educate policymakers and industry stakeholders on content best practices and assert the value of intermediary liability. A coalition will enable technology companies to develop common positions on content regulation, initiate engagements and share their knowledge and understanding of technology with governments. By sharing information in an open and transparent forum, the technology

industry can bring policymakers into the digital economy and build trust through these coalitions. The technology industry can impact global discussions on content regulation, encourage informed debates and in turn, facilitate a global and accessible digital economy.

Now is the time to drive these efforts as governments around the world are focused on countering the spread of disinformation, particularly regarding COVID-19 and public health. A coalition can work closely with policymakers to ensure the creation of regulations that will encourage the flow of information and data, while avoiding burdensome compliance requirements and potential over-regulation.

We lead countries to fair tech

Access Partnership is the world's leading public policy firm that provides market access for technology. Our team uniquely mixes policy and technical expertise to optimise outcomes for companies operating at the intersection of technology, data and connectivity.

9th Floor, Southside
105 Victoria Street
London SW1E 6QT
United Kingdom
Tel: +44 (0) 20 3143 4900
Fax: +44 (0) 20 8748 8572

www.accesspartnership.com

AccessAlerts

AccessPartnership