RSIS | S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS COMMENTARY

www.rsis.edu.sg

No. 170 – 23 November 2023

Regulating Online Harms: Are Current Efforts Working – Or Even Workable?

By Sean Tan

SYNOPSIS

Rapid digitalisation has occurred in tandem with the amplification of online harms. The spread of malicious online content and activity poses an even greater danger to vulnerable users. But how should security guidelines for digital platforms – or indeed, the Big Tech companies – be implemented?

COMMENTARY

The extending reach of digital applications offers new opportunities, but also heightens the potential for various social harms in online spaces. Any optimistic long-term visions for emerging technologies are at odds with real and pressing online safety issues. Many harmful online phenomena – including those which threaten national security, such as violent extremism and disinformation – are in fact abetted by digital growth.

Some of these threats may appear unprecedented. Early developers of digital communication networks did not anticipate their eventual scale of expansion, much less their exploitation for cybercrime such as scams, harassment and sexual abuse. Since the advent of the global Internet, authorities around the world have steadily become more vigilant to these dangers. Even so, the constantly evolving nature of online harms and digital technology poses a challenge for regulators.

Shifts – and Similarities – in the Global Online Regulation Landscape

The accompanying evolution of laws dealing with online harms has shown that regulation has been far from straightforward. Nascent efforts, such as Title V of the United States' 1996 Telecommunications Act, and Malaysia's Communications and Multimedia Act of 1998, were early attempts to regulate the Internet, including the criminalisation of offences involving inappropriate online content. However, in more recent years, the dramatic advancement and proliferation of digital technology has reshaped perceptions of online risk, prompting far more extensive safety measures.

A prominent feature of modern legislation is the imposition of new requirements on digital service providers. Recent examples include the United Kingdom's Online Safety Bill and Singapore's Online Criminal Harms Act, both of which contain stipulations for digital platforms believed to host illicit online activities. In 2022, Malaysia extended the scope of its Communications and Multimedia Content Code to include online service providers, before recommending additional provisions for online platforms last September.

These requirements are typically paired with compliance mechanisms. For instance, the US Digital Consumer Protection Commission Act proposes an overarching regulatory structure for Big Tech companies, including an independent regulator whose practices would mirror that of existing consumer protection agencies. A similar independent online safety regulator has operated in Australia since 2015.

Perhaps the most ambitious regulatory instruments today are the European Union's Digital Service Act and Digital Markets Act. Both have superseded existing legislation in EU member states. They target a comprehensive range of online services and harms, and are chiefly aimed at the world's largest technology companies.

Though these measures inevitably differ to some extent, some common strands are identifiable. There is a general consensus on certain forms of unacceptable content and activity, such as encouraging terrorist acts, sexual harassment, and inciting hate and violence. An especially clear red line relates to child exploitation and abuse. Many child advocacy organisations – deeply familiar with the dangers in digital spaces – have expressed support for and requested additional amendments to the relevant laws. There is an increasing shared perception of online harms as an acute and immediate threat. Many initiatives and proposals emphasise the need for substantial and urgent action.

Potential Areas of Oversight and Concern

However, despite their lofty ambitions, it is yet to be seen if these measures and regulations can be meaningfully implemented in practice, or if they are indeed feasible. Of notable concern is a seemingly limited understanding of technology among policymakers – in particular, those who advocate for a proactive, hands-on approach to content moderation via the use of software tools to detect harmful content, such as client-side scanning.

While this approach may, at a glance, seem appropriate given the importance of protecting vulnerable groups, experts have since questioned whether it is technically possible to detect harmful online content without bypassing end-to-end encryption – a security measure integral to user privacy. Although states such as the UK have since indicated that they will not deploy client-side scanning, such proposals nevertheless set a dangerous precedent. In fact, any plans to bypass encryption are likely to be problematic for all users, but especially so for at-risk individuals.

Also worrying, technological illiteracy on the part of policymakers raises questions over the enforcement of accountability for Big Tech companies. This is especially the case where safety provisions and obligations are of a technical nature. Any uncertainty or vagueness in the definition of key terms would almost certainly make policy formulation and implementation less effective, given that independent regulators may also struggle to interpret important definitions.

Moreover, a detailed knowledge of relevant technologies is increasingly vital, as the continued growth of emerging technological tools threatens to further complicate regulatory efforts. These developments cast further doubt on the suitability of ambitious and overarching regulatory proposals designed to tackle several complex – and evolving – issues at a single given time.

What should be done?

Ultimately, aspirational measures to tackle online harms, no matter how laudable, will only be as strong as their legal enforcement.

While some authorities seem to be taking comprehensive and decisive action against online harms, this can mask a rudimentary understanding of important issues. On the contrary, a failure to engage with these issues thoroughly can create further risks to civic safety. Any attempts to expand the scope of regulation must be paired with sufficient technical knowledge, in order to avoid unintended consequences. Challenging dialogues between governments and industry experts are an inevitable, but much-needed step not only in the knowledge sharing process, but also in helping to build relationships and transparency in the long-term combatting of online harms.

Additionally, the proliferation and transformation of online harms and digital technology is almost certain to outpace policy development. In dealing with the most distinct threats, policymakers may wish to adopt a more incremental and adaptable strategy, which would then make it easier to adjust course should the nature of these threats subsequently change.

This iterative approach is by no means without drawbacks, as overall progress on regulation would likely be slower. However, policymakers who have the relevant technical knowledge would be better equipped to anticipate new risks. At a certain level, policymakers armed with the requisite expertise may even work to hold Big Tech companies accountable at the product design phase, before new services are released to the general public.

Sean Tan is a Senior Analyst at the Centre of Excellence for National Security (CENS), a constituent unit of the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore. Prior to joining CENS, he was based at NTU's Centre for Information Integrity and the Internet (IN-cube), a research centre that aims to help promote information integrity in online spaces.