3 Key Issues In UK's 'Online Harms' Regulatory Framework

MAY 28, 2019

This article first appeared on Law360 on 24 May 2019.

How do you police the internet? That is the question that the government sought to answer with the launch of last month's online harms white paper.[1] The white paper, a cross-departmental collaboration between the home secretary and the culture secretary, outlines a proposed regulatory framework to tackle the prevalence of illegal and harmful content online, dubbed "online harms."

The concept of "online harms" is a broad one, going further than illegality (which would include, for example, content relating to child sexual abuse or terrorism) and encompassing "harms with a less clear definition" such as trolling, disinformation and advocacy of self-harm. Currently, such harms proliferate on internet platforms which are effectively self-regulating. That may be about to change.

The government plans to impose a statutory duty of care on companies to protect its users from harmful content which may be hosted by its platform. Breaches of this duty of care will be investigated and sanctioned by a dedicated regulator, and the penalties commensurate with the severity of the breach.

Within the wider debate around the effect that such regulation may have on freedom of speech, three key issues arise regarding the enforcement of the proposed duty: firstly, there is the need for an independent regulator which is both sufficiently funded and staffed with those who have the requisite expertise; secondly, there is the issue of the proposed penalties and their effectiveness; and finally, the problem of the U.K. establishing jurisdiction where content can be accessed by the click of a button anywhere across the globe.

A New Regulator?

The white paper outlines the need for an independent regulator to implement, oversee and enforce the new regulatory framework. Whether this will be an entirely new body, or whether the responsibilities will be taken on by an existing regulator — although it is unclear who might be up for the job — one thing is obvious: the task will not be an easy one. As well as uncovering, investigating and sanctioning breaches of the new duty of care, the regulator will be tasked with broader responsibilities to "promote education and awareness-raising about online safety, and to promote the development and adoption of safety technologies to tackle online harms."

In times of tightening budgets and overstretched resources, a key consideration will be the staffing and funding of the regulator eventually given the task. Regulating such a technically complex industry requires a deep understanding of how that industry works; individual platforms and services present their own unique nuances and challenges. Investigation and enforcement actions will need to be carefully and thoughtfully crafted.

Such expertise is not available freely and does not come cheap, but will be critical to the success of this bold venture. The white paper proposes that the regulator will be funded by the industry it regulates. Although this idea is not a new one — the Financial Conduct Authority and Prudential Regulation Authority are funded by the financial services and banking firms they oversee — imposing such a tariff on companies which are already well established and wield significant power may be an uphill battle.

What Might the Penalties Look Like?

Of course, a new regulatory framework means nothing if the regulator cannot impose penalties for breaches in order to effectively incentivize compliance. The white paper acknowledges that these sanctions need to be not only strong enough to deter breaches (while still being proportionate to the harm caused), but also capable of applying to a huge variety of different companies and platforms. A number of potential options are proposed, some of which are to be expected — for example, civil fines where the duty of care has been breached.

There is also a suggestion of a public “naming and shaming” in cases of a proven breach. In an industry where consumer power is everything, the threat of such reputational damage could prove persuasive. On the other hand, it could perhaps be argued that platforms hosting “harmful content” would not be affected by such a notice because its users tend to actively seek out such content in the first place.

However, the white paper also suggests that stronger powers may be needed in cases of particularly serious harm. The nuclear option would be ISP blocking, which would essentially prevent U.K. users from accessing a platform. While this is stated to be a penalty of last resort in cases of the most egregious and repeated failures to address illegal (rather than just harmful) content, many have suggested that such blanket exclusions could amount to state-sanctioned censorship.

A parallel may be drawn with the financial services industry, where the FCA has the power to withdraw permission to perform regulated investment activities where a company continually breaches regulations and is posing a danger to consumers. However, two crucial distinctions can be drawn.

Firstly, the FCA must authorize these activities in the first place, and is thus fully entitled to remove such authoritative; no such permission is needed for online platforms to operate. Secondly, and more importantly, blocking an online platform has the potential to infringe freedom of speech in a way that preventing a firm from providing financial services simply does not.

A second option suggested is the imposition of civil, and possible criminal, liability for individual

senior managers in order to hold them personally accountable for major breaches of the duty of care. It is envisioned that this system would work in a similar way to the Senior Managers & Certification Regime introduced in the financial services industry three years ago in an attempt to drive cultural change.

The immediate difficulty with this proposal, as it was with the SMCR, is that it could prove too burdensome and may put people off assuming senior roles in these companies for fear of being held accountable for every problem occurring in their field of responsibility. The nature of online platforms adds a further complication: while individuals within the SMCR are an employee of a company tasked with controlling other employees of the same company, senior individuals at an online platform will, effectively, be ultimately responsible for policing the postings of the general public. This is no mean feat, and one which may prove too big an ask for many.

The key when designing and imposing these penalties will be proportionality. The threat of such damaging sanctions may push companies to err too far on the side of caution, removing content which may toe the line between “acceptable” and “harmful” because they take the view that it is simply not worth the risk. The potential impact on the freedom of the press and the freedom of speech could be devastating. Enforcement of the proposed regulatory framework will be a delicate exercise, attempting to balance protection of the public with fundamental rights.

Jurisdictional Hurdles

One obvious hurdle which the white paper does not adequately address is the issue of jurisdiction. The internet, by its very nature, is a global phenomenon and often a company cannot be pinned down to one particular country: its jurisdiction of incorporation, primary place of business and server hubs may be scattered across the globe.

The white paper attempts to get around this by asserting that the new regulatory framework will be drafted to catch any company which provides a service to U.K. users. This is a vague proposition, generating more questions than answers — for example, does harm have to have been caused to U.K. users for it to be investigated and, if so, will there be a threshold of harm which must be met before the U.K. authorities can bring enforcement action?

Pinning liability to particular senior individuals may be one way of getting around this. If a breach occurs on a person’s watch while he or she is physically situated in the U.K., this could provide a more convincing jurisdictional hook. However, this would have an almost inevitable chilling effect on the attractiveness of the U.K. as a place to do business; companies could become incredibly reluctant to have a physical presence in the jurisdiction if its location came down to a choice between engaging or avoiding such liability.

Even where the U.K. is able convincingly to establish jurisdiction, the global nature of the internet means that any investigation or enforcement action has the potential to infringe on the sovereignty of regulators in other jurisdictions. There could be outcry if the U.K. attempts to sanction a U.S. platform where the U.S. itself has made no move to curtail or punish so-called harmful activities.

At the very least, investigation and enforcement will require a high degree of cooperation and

collaboration between international regulatory bodies. With Brexit looming, these issues will become even more pressing as formal cooperation mechanisms fall away.

A Balancing Act

The need for regulation in this industry has long since been recognized, and the U.K. is the first jurisdiction to take such bold steps in outlining a plan to achieve that. But these steps are walking on a tightrope: the tension between protection of the public from harm and protection of freedom of expression, coupled with the need to preserve the U.K.'s reputation as an attractive place of business, means that there is a very fine balance to be struck.

However, it must be remembered that these proposals are in their infancy. With effective consultation, the government may very well be able to develop a comprehensive and coherent regulatory framework which is fit for purpose. The key lies in recognizing dangers at the outset of the legislative process to ensure that the particular sensitivities of this industry are properly dealt with. Haphazard and thoughtless regulation could do more harm than good.