INTERNATIONAL SOCIAL MEDIA ASSOCIATION

The global voice of social media law

Online Harms White Paper Response

Submitted on 1 July 2019

Prepared by: Nick Boyce, Jack Zhou and Calvin Fang

The International Social Media Association (ISMA) is a not-for-profit organisation dedicated to harmonising legislation and policies on a global scale, and to provide education and information. Our mission is to advance, protect and balance the rights of businesses and individuals on the digital platforms which are used every day.

Responses to Online Harms White Paper

Question 12: Should the regulator be empowered to i) disrupt business activities, or ii) undertake ISP blocking, or iii) implement a regime for senior management liability? What, if any, further powers should be available to the regulator?

i) Disrupting business activities

As a general proposition, the regulator should not be mandated to disrupt business activities, even as a form of deterrence in response to behaviours which are deemed contrary to the purposes of the regime contemplated by the White Paper. However, depending on the powers of the regulator, disruption of business activities may be a collateral consequence of exercising its function. In respect of regulating social media platforms and services, content is principally user generated. If the regulator was able to unilaterally impose restrictions on the way users create or share content on platforms then this could fundamentally undermine the platform itself, and accordingly, its business activities. Such intervention from the regulator would have the undesired effect of compromising user confidence in social media use and the United Kingdom may be perceived as a jurisdiction where there is excessive interference with individuals' online activity. To the extent that "business activities" (however defined) breach the law, there are already existing legal mechanisms in place to prevent and/or halt these activities. Accordingly, any action taken by the regulator which may have the effect of disrupting business activities needs to balance the public interest in preventing online harm against the public interest in maintaining a jurisdiction which promotes commercial activity and fosters online innovation.

ii) Undertaking ISP blocking

In many jurisdictions (including Australia and the United Kingdom), ISP blocking ordinarily requires an application to a relevant court or judicial body (for example by way of injunction). Giving the regulator the power to undertake ISP blocking risks creating an excessive concentration of power. We acknowledge that seeking orders from a judicial body can be a timely process, however, there needs to be a balance between expediency and ensuring that a fair and transparent process is followed. Options should be explored to develop a mechanism for the regulator to have an expedited process to make judicial applications. Further, the regulator should have a system whereby requests can be made directly to private companies and platforms to voluntarily remove content. It is important for maintaining public confidence in democratic principles that a state body is not perceived to have excessive powers of censorship.

It is also important to note that ISP blocking can be circumvented by, for example, the use of VPNs and therefore consideration should be given as to the effectiveness of this action in efficiently reducing the risk of online harm.

iii) Regime for senior management liability

The rationale behind introducing a senior management liability regime appears to be solely to put pressure on the key decision makers within internet and social media companies to ensure that their companies are compliant, and that appropriate measure are put in place to prevent online harm. Similar liability regimes operate across different jurisdictions for ordinary companies whereby senior management can be liable for the activities of their companies and their officers. However, it is important to recognise the lesser level of control that social media platforms have over their users. There is no formal relationship, such as in an employment or contractual relationship, under which the senior management can exercise such a high level of control over user-published content. While the penalty regime may encourage companies to improve their content management processes to a very limited degree, there are already sufficient drivers (e.g. public perception, brand image) to encourage this. In any case, even if a senior management penalty regime existed, it seems unlikely that it would be enforced as this would arguably discourage social media and internet companies

from conducting their operations in a jurisdiction where this type of penalty regime operates frequently.

Question 17: Should the government be doing more to help people manage their own and their children's online safety and, if so, what?

One obvious course that the government can take to manage people's online safety is through legislation. The White Paper contemplates an accountability regime for private companies (and senior individuals within those companies) to ensure that they have adequate systems in place or take sufficient steps to manage the safety of their users and other internet users generally. This is certainly an approach which has been adopted in other jurisdictions. In Australia, in April of this year, the Federal Parliament enacted the *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019*, which greatly increased the penalty regime for platforms which fail to take down or block access to (what is deemed) violent or abhorrent material. The legislation has been heavily criticised for failing to tackle the underlying issues, for being potentially unenforceable, incentivising excessive content monitoring, and having a potentially chilling effect on freedom of expression. Where user generated content is the source of online harm (as opposed to content created by the platforms), a more pragmatic form of government intervention would be increased education, as opposed to implementation of a deterrent regime.

While it is undisputed that the government has a role in providing free and easily accessible tools to promote education and awareness, the way in which this is approached requires real consideration. There are already numerous government initiatives across a number of jurisdictions with the purpose of increasing awareness and educating people about online safety and how to avoid online harm, particularly with a focus on targeting young people. For example, the Australian Office of the eSafety Commissioner offers practical guides and tips for parents and carers, in addition to offering various channels to help deal with cyberbullying and manage reporting of (what is deemed) offensive or illegal content. However, most of these initiatives currently take an "opt-in" approach. That is, many helpful and valuable tools are available to internet users who choose to access them. While this is a positive step, it does not get anywhere close to achieving the level of universal education and awareness necessary to ensure that the internet is a safe space for all. For that reason, the government should

explore the option of mandatory or "embedded" education systems. We have explored this concept further in our response to the next consultation question.

Question 18: What, if any, role should the regulator have in relation to education and awareness activity?

It is evident that more needs to be done to educate people about online harms, and how to protect themselves and their dependents. This has been identified as a key area of focus by the White Paper. The regulator should certainly have a role in relation to promoting education and awareness. One obvious reason for the regulator exercising this role is the necessary relevant expertise that the regulator and its delegates will hold in order to exercise their functions. Further, as with other regulatory bodies, it is incumbent upon that body to inform and advise the public about the regulator's role, powers and the activities which it regulates. Taking that into account, while the regulator should have some role to play in education and awareness, there will be limits (both due to resourcing and practical constraints) as to the extent of its reach.

Accordingly, the task should not fall solely within the remit of the regulator. It is also incumbent upon private companies (e.g. social media platforms, ISPs) to develop their own education initiatives. These should aim to not only ensure legal compliance but also to develop best practice systems. Educational institutions (such as schools and to a lesser extent tertiary institutions) should also be responsible for education relating to online safety and prohibited behaviours, much in the same way that they often do in relation to awareness around discrimination laws and avoiding discriminatory behaviours. As raised in the previous response, proportionate government intervention should be explored as an appropriate measure for achieving mandatory education which will reach as wide an audience as possible. This can be achieved easily by building in compulsory units into the national curriculum. Additionally, the government should also explore joint initiatives with large social media and internet companies whereby training and education modules can be "embedded" into the user experience. For example, instead of private companies trying to change behaviours by amending their terms of use, the regulator (or other appropriate government department) can work with these companies to develop educational tools which users will have to engage with during their use of the relevant platform. This will not only foster collaboration between

the regulator and private companies, it will also ensure that all users receive a minimum level of online awareness training, not just those who independently seek out information or guidance. While not completely analogous, this is similar to measures taken by financial services regulators across the global industry whereby employees or service providers at financial services companies are required to undertake AML and CTF training.

Submitted Online: 1 July 2019