Proposed online UK safety measures to support innovation and a thriving digital economy

A paper to inform and provide guidance for risk management and insurance professionals

THE CONTEXT AND PURPOSE OF THIS PAPER

The world is increasingly volatile, uncertain, complex and ambiguous. Businesses must move faster, drive innovation, and adapt to and shape their changing environment. The pressure to manage and report risks has never been greater. Consequently, boards and business leaders operate in an increasingly unforgiving environment and need a defined approach and the support of professionals fit to help them fulfil their risk oversight responsibilities. Companies that can depend on their boards to deliver this oversight across the spectrum of risks have an advantage. Whilst, at face value, practices for managing risk might seem unaffected by this context, the underlying business dynamics of today are so different from those of the past, they trigger the need for recalibrating risk management and rebalancing the effort between managing traditional risks and emerging risks.

The Online Harms White Paper consultation published by the Department for Digital, Culture, Media and Sport sets out the UK Government's plans for a world-leading package of online safety measures that also supports innovation and a thriving digital economy. This package comprises legislative and non-legislative measures, and is intended to make companies more responsible for their users' safety online, especially children and other vulnerable groups. The White Paper proposes establishing in law a new duty of care towards users, which will be overseen by an independent regulator. Companies will be held to account for tackling a comprehensive set of "online harms", ranging from illegal activity and content to behaviours that are harmful but not necessarily illegal.

The purpose of this Airmic paper drafted with law firm BLM, is to provide information about the Government's intent for this regulation, Airmic's response to the Government consultation, to outline the next steps in the consultation process and to inform the risk professional when engaging and collaborating on this subject with their governance, information and technology peers.

1. WHAT IS "ONLINE HARM"?

The online environment is increasingly becoming a very real part of our offline lives, delivering breaking news, helping us to maintain friendships and join in on conversations on issues that affect us, and the technology has become central to a wide range of business processes. With nine in ten UK adults and 99% of 12 to 15-year-olds online, this trend isn't going away, and with new technology becoming available to meet the constantly changing and escalating needs of its users, the true 'reach' and impact of our online activity is only now beginning to manifest itself, both in relation to users and wider society.

Much as technology is often seen as agnostic, its users tend to be more partisan. Over the past five years or so, we've seen examples of where the internet and social media can be used to spread terrorist content and ideology, undermine otherwise civil conversations and allow for the direct harassment of other users. It's fair to say that the social media genie is out of the bottle, and many users are still getting to grips with the effects and consequences of their online activity as related ethical and moral standards continue to develop.

The next generation of technology, such as AI and machine learning, while enormously powerful in terms of helping people, also opens-up new potential harm, such as exacerbating inherent biases in society and impacting on individual privacy.

It's against this backdrop, the UK Government has sought to get to grips with what it describes as "help to shape an internet that is open and vibrant but also protect its users from harm" and "taking decisive action to make people safer offline". To that end, the Online Harms White Paper was published on 8 April 2019, and the consultation on its content ran until 1 July 2019.

We'll get into the issues and the legislative challenges that the White Paper raises in further detail below, but the initial list of "online harms" in scope were broken down into three groups:

Harms with a clear definition

- Child sexual exploitation and abuse
- Terrorist content and activity
- Organised immigration crime
- Modern slavery
- Extreme pornography
- Revenge pornography
- Harassment and cyberstalking
- Hate crime
- Encouraging or assisting suicide
- Incitement of violence
- Sale of illegal goods/services (such as drugs and weapons)
- Content illegally uploaded from prisons
- "Sexting" of indecent images of under 18-year-olds (creating, possessing, copying or distributing indecent or sexual images of children and young people under the age of 18).

These harms are clearly defined because there are criminal and civil legal sanctions in place to deter them, and attendant mechanisms for individuals or law enforcement to either force such content to be taken down from online platforms or to obtain further information to pursue those responsible for it. That said, with police resources stretched, and fewer police officers trained and able to deal with offences of this nature and individual remedies being technical in nature and expensive to pursue through the civil courts (often involving jurisdictional and other complex legal issues), a clear definition in UK law only solves part of the problem.

Harms with a less clear definition

- Cyberbullying and trolling
- Extremist content and activity
- Coercive behaviour
- Intimidation
- Disinformation
- Violent content
- Advocacy of self-harm
- Promotion of female genital mutilation.

These harms are more commonplace than the first group and, in some cases, may raise free speech issues, notably around "trolling". Whilst many users may feel at least partly immune to this kind of "harm", the effect on others can be profound – the Crown Prosecution Service (CPS) guidance on communications offences refers to the balance between harmful content and freedom of expression, and this will be one of the key battlegrounds involved in the shaping of the new regulatory system likely to come out of the White Paper's consultation. Notably, "fake news" is seen as a form of harm equivalent to some other more direct and impactful acts.

Underage exposure to legal content

- Children accessing pornography
- Children accessing inappropriate material

This is one of the key drivers behind the White Paper. The UK's Age Verification System introduced in the wake of the Digital Economy Act 2017 for the viewing of pornographic material has served as an illustration of the difficulty involved in regulation of this nature, with the proposed system being delayed several times due to "administrative errors". The level of availability of this type of content in an unregulated environment is one of the most pressing reasons behind the White Paper, and what may follow. Some of these harms are already effectively regulated, either through legislation or codes of practice, but the newer, developing harms are now arguably seen to be so problematic by the general population and Government, that something must change. The White Paper describes the current regulatory framework as "fragmented" and it is widely seen as not fit for purpose in the digital world.

2. WHY NEW MEASURES ARE NEEDED AND WHY THE UK IS BLAZING THIS TRAIL

Given its global nature, regulating the online environment is at best a challenge and at worst an impossible dream. Since social media became a truly pervasive part of the everyday lives of many individuals, there are many examples of old law (both civil and criminal) struggling to keep pace with this new technology, and of users not understanding the effect that their posts can have upon their recipients. Additionally, where EU and UK law has tended to protect platforms and companies from the lion's share of liability arising from content posted or disseminated using their systems, Facebook, Google and others are coming under increasing and very public pressure to do more to ensure the safety of their users from "online harms". In the wake of several very public cases involving the suicides of young people, the UK Government has acted to try and deal with the problem head on.

3. LINKS TO OTHER REGULATIONS

Beyond the White Paper, the General Data Protection Regulation (GDPR) and Data Protection Act 2018 are now in force and beginning to force changes in relation to the use of personal data and individual privacy, and the EU's Audiovisual Media Service Directive (which may well never come into force in UK law in the wake of Brexit) proposes huge fines for services hosting harmful video content online. Certainly, regulation of the technological environment is nothing new, but the sheer scope of what is proposed in the White Paper looks to redefine the relationship between the Government, the UK population, social media itself and the businesses which form part of its DNA. Much as the Law Commission is also working to clarify the operation of criminal law online, there is a perceived gap in consumer protection as regulated by the Competition and Markets Authority (CMA) online, and this is what the new regulatory landscape would look to fill.

Many of the platforms involved have either encouraged or welcomed further oversight, but much as there have been several very well-intentioned attempts to self-regulate and set best practice, the admission of platforms

such as Twitter and Facebook that they have a "trolling problem", amongst others, means that many now see further regulation as not only inevitable but a cost of doing business in the United Kingdom.

4. THE IMPLICATIONS FOR ORGANISATIONS AND THEIR GOVERNANCE

Perhaps the most controversial of all of the White Paper's proposals is the introduction of a new statutory duty of care on relevant companies "to keep their users safe and tackle illegal and harmful activity on their services". The proposal is that this be enforced by the new "Online Harms Regulator". Compliance will be linked to a "risk-based approach", proportionate and underpinned by new codes of practice to flesh out the new requirements.

The new regulatory framework will apply to "companies that provide services or tools that allow, enable or facilitate users to share or discover user-generated content, or interact with each other online". Whilst it is tempting to assume that this definition was drafted with the likes of the big multinational media companies, the White Paper recognises that "these services are offered by a wide range of companies, including start-ups and SMEs, and other organisations such as charities". However, there will also be a commitment to "minimise excessive burdens, particularly on small business and civil society organisations". Many smaller businesses may offer services of this type as an adjunct to their main activities and are unlikely to welcome even more 'red tape'.

Given its status, the current scope of the White Paper and its consultation were very broad and have generated significant uncertainty around terms such as "facilitation", what counts as a "public channel" and whether a standard forum site containing a public comments section would fall within scope. Whilst many organisations will want to begin their contingency planning now, it's fair to say that the current proposals only represent the first step on what could be a journey of a thousand miles. The current picture is, by its very nature, incomplete – the "culture of transparency, trust and accountability" it seeks to create is similar to the requirements of the GDPR and Data Protection Act 2018, with which many businesses are still struggling to cope. The Information Commissioner's Office (ICO) has worked hard to fill in gaps and promulgate best practice, but it is also only now getting to grips with the issues raised by the online advertising industry, a far more substantial challenge when confronting an entire sector built on the exploitation of personal data relating to internet users.

Additionally, introducing a new standard or "duty of care" that could give rise to civil claims (notably, the ability to issue a civil claim more easily in the event of a data breach as introduced by the GDPR only came after several notable Court decisions effectively recast the Data Protection Act 1998) could prove extremely problematic, not least in the event that it covers all of the various "harms" listed above. The Court is currently wary of creating a flood of data breach claims and the Government is unlikely to encourage a new industry in claims arising from apparent "online harms".

This could become a key area of focus for an "Online Harm Officer" and is it worth considering whether that role might naturally fit alongside an existing role, such as the Data Protection Officer who will have many of the same skills?

Certainly, regardless of whether the new duty of care materialises as intended or regulation proves as punitive as may be suggested, even a new self-regulatory environment will give rise to new risks to match the evolving rewards of the online environment. Although many businesses may have been through a similar exercise when preparing for the GDPR, organisations may now want to consider appointing a separate 'Harm Officer' to be prepared for the new regulatory environment. What the White Paper does immediately is move the various "online harms" further up the corporate risk register, although a fuller response to that reclassification will only be possible in the wake of clearer guidance from the new Regulator.

5. WHY RISK MANAGERS AND INSURANCE MANAGERS SHOULD BE INFORMED AND WHO THEY SHOULD BE COLLABORATING WITH

The UK has long sought to make itself "the safest place in the world to be online". The Online Harms White Paper and subsequent consultation has sought to set out the Government's intention to use "legislative and non-legislative measures" to make companies more responsible and accountable for their users' safety online – especially children and vulnerable groups – through a "world-leading package of online safety measures that also supports innovations and a thriving digital economy".

Airmic supports establishing in law a new duty of care towards users, which will be overseen by an independent regulator. We believe that the scope in terms of what is harmful and who decides, the definition of data itself, the definition of language and the definition of in-scope companies all require further clarification. As regards in-scope companies, without this clarity, many companies will face uncertainty and there is a risk of 'mission creep' and/or vexatious action.

6. HOW THE REGULATION MIGHT WORK AND WHEN

Beyond the commitment to a proportionate and risk-based approach, it's likely that the new regulatory environment will, unless policed by the service providers and platforms themselves, follow a similar blueprint to the GDPR and Data Protection Act 2018. The current

proposals relating to fines for breach of the Audiovisual and Media Services Directive suggest that the harshest fines for the worst offenders will be of a similar level, although bringing further clarity to a very wide-ranging set of proposals will take some time even if legislation is introduced in 2020.

The consultation closed on 1 July, and the current Culture Secretary, Jeremy Wright, has indicated that new legislation will be introduced "as soon as possible next year", alongside the establishment of an independent regulator (which may be OFCOM, another existing body or a new body) to enforce a risk-based approach to priorities to tackle activity or content where the risk of harm to users is most acute.

7. AIRMIC AND THE CONSULTATION

Airmic supports establishing in law a new duty of care towards users, which will be overseen by an independent regulator. We believe that the scope in terms of what is harmful and who decides, the definition of data itself, the definition of language and the definition of in-scope companies all require further clarification. As regards in-scope companies, without this clarity many companies will face uncertainty and there is a risk of 'mission creep' and/or vexatious action. The issue of in-scope companies is of particular concern to our members – the definitions in the White Paper are very broad, and Airmic is worried that its members will find themselves in scope even when they are not in the sectors that the White Paper is primarily directed at – this includes which companies will be expected to help pay for the day-to-day operations of the regulator. We also believe that clarity on these issues should form part of the consultation and development process, and be debated alongside the legislation, rather than after the legislation is passed and consequently left to the regulator to decide afterwards.

Airmic concluded that there should be a balanced approach that recognises the need for some new regulation alongside other measures, such as education and an element of self-regulation by the industry, which should still have its place. Airmic recognises the positive benefits of operating in regime where consumers feel safe.

There is potentially some competitive advantage for the UK if the UK can demonstrate that we have achieved the balance between innovation, freedom, and protecting people. Is there an equivalent at the individual company level – manging the negative and converting the positive?

8. TAKEAWAYS

i. Organisations should familiarise themselves with the papers published by UK.Gov and consider whether they are likely to fall "in scope" of the proposed new "online harms" regime
ii. Through a multifunctional team, including Legal, Human Resources, Information, Technology, Compliance, and Risk Management and Insurance, organisations should consider the implications of their organisation being "in scope"
iii. Organisations should consider how this subject may touch other stakeholders, including those in their supply chain, and their contract terms
iv. Organisations should consider creating a single point of contact with responsibility for dealing with the new regulatory regime, whatever final form it may take
v. Organisations should consider to what extent their content and activities fall within the scope of the proposed new regime and whether they wish to continue providing them
vi. Under the leadership of the organisation's Data Protection Officer, organisations should carry out a risk assessment, similar to a Data Protection Impact Assessment (DPIA), to get a clear idea of which of their activities may cause "online harm"
vii. Organisations should map their current insurance cover to identify any gaps in coverage and any coverage which may protect them from future claims relating to "online harm", as well as clarifying the scope of cover for regulatory fines
viii. Organisations should monitor relevant developments and include these in their overall approach for horizon scanning
ix. Organisations should brief their C-suite and board and keep them updated