



techuk.org | [@techUK](https://twitter.com/techUK) | [#techUK](https://hashtech.com/techUK)

techUK response to Ofcom video-sharing platform regulation call for evidence

September 2020

10 St Bride Street
London
EC4A 4AD

T 020 7331 2000
F 020 7331 2040
www.techuk.org

techUK | Representing the future

About techUK

techUK represents the companies and technologies that are defining today the world that we will live in tomorrow. The tech industry is creating jobs and growth across the UK. More than 850 companies are members of techUK. Collectively they employ more than 700,000 people, about half of all tech sector jobs in the UK. These companies range from leading FTSE 100 companies to new innovative start-ups. The majority of our members are small and medium sized businesses.

Introduction

techUK supports the objectives of the video-sharing platform regulations set out under the AVMS Directive. Industry is committed to fulfilling its roles and responsibilities, protecting young people from harmful content and all users from illegal content and that which seeks to incite hatred and violence.

While the current VSP regulations will only initially effect a small number of companies in the UK, with Ofcom expected to gain additional responsibilities under regulatory proposals around online harms the experience learned from its implementation will be critical to creating a proportionate, reasonable and effective framework. In addition, uncertainty around the UK's future relationship with Europe leaves open the possibility that more companies than currently anticipated could find themselves in scope of the regulation at a later date.

techUK supports the UK Government and Ofcom's approach to the implementation of VSP regulations. Adhering to the minimum requirements of the Directive is the right approach to take as these issues are already under advanced consideration and consultation through other initiatives, including the proposed online harms framework. We also warmly welcome Ofcom's commitment to work constructively alongside industry and build an approach that relies on robust evidence and an understanding of the current capabilities of different services.

techUK will not seek to answer every question outlined in its response to the consultation. Many questions relate to the specific way in which VSPs operate their platforms and rely on data and information not available to techUK and better gathered through Ofcom's direct relationship with industry operators. Instead, we will seek to focus on the broader industry perspective highlighting some best practice and principles we hope will help create an effective framework that can be built on for the future.

Systems and Processes

- **Question 19: What examples are there of effective use and implementation of any of the measures listed in article 28(b)(3) the AVMSD 2018?**

Industry is committed to tackling harmful content that appears online, constantly investing in people, partnerships and technology to improve the response to these challenges over time.

In recent years investment committed to trust and safety has vastly increased, with some platforms now hiring tens of thousands of individuals in this space. Last year, Facebook announced it was spending \$3.7bn on safety and security, the same amount as the company's total revenue at the time of its IPO. TikTok, a relatively new entrant into the sector, has announced it already has over 10,000 people working on trust and safety.

This investment is matched by a commitment to partner with key stakeholders at a national and international level. Partnerships are crucial to effectively keeping users safe online, and are involved in many of the measures listed in Article 28(b)(3), including the development of terms and conditions, or reporting mechanisms.

For example, the vast majority of platforms now operate 'Trusted Flagger' programmes. These programmes enable law enforcement, civil society, charities and other important and reliable stakeholders to alert platforms to harmful or violating content with a fast-tracked review process.

These partnerships are also used in the development of terms and conditions. In September 2020 the Samaritans [published new guidelines](#) to support sites hosting user generated content on how to safely manage self-harm and suicide content and keep vulnerable people safe online. These guidelines were developed in collaboration with industry including Facebook, Instagram, Google, YouTube, Twitter and Pinterest, as well as government, academics and third sector organisations to help tackle the issue, whilst improving access to content that can be a source of support.

Investment in technology is also a key part of this challenge, with industry constantly investing in new tools to better identify, remove and disrupt the spread of harmful content online. This includes the development of AI and machine learning to proactively search for content which breaches terms and conditions before it is seen by anyone.

This investment also leads to better parental controls over the use of platforms. There are currently a range of technological solutions available to parents to control the use of devices and applications by children and young people. For example, Google's Family Link enables parents to create a Google account for their children under 13 and parents can use the app to manage aspects of the account and their child's single device. Microsoft allows parents to set daily and weekly usage limits on both the Xbox console itself and content on Xbox Live. Apple's iOS has Digital Wellness, allowing people to see how much they use their phone and set limits of usage, notifications and even schedule downtime.

Many platforms also run extensive media literacy initiatives to empower their users to have better control over their online experience, and enabling them to critically assess and evaluate content, in addition to boosting and understanding of the actions to take if they encounter troubling content. For example, TikTok runs its own Safety Centre which provides information, advice, tools and resources on safety features and where to learn more about the platform. This includes a specific Youth Portal to build digital literacy in young people, for example around privacy or community best practices.

Keeping Users Safe

- **Question 21: What indicators of potential harm should Ofcom be aware of as part of its ongoing monitoring and compliance activities on VSP services?**
- **Question 22: The AVMSD 2018 requires VSPs to take appropriate measures to protect minors from content which 'may impair their physical, mental or moral development'. Which types of content do you consider relevant under this? Which measures do you consider most appropriate to protect minors?**

Keeping its users effectively safe online is the priority for industry, and we recognise that good regulation and standards can be an effective enabler of innovation and commerce. Successive steps have been taken over recent years as the amount of online content has grown and there is a commitment across industry to crack down on content which is not simply illegal, but harmful as well.

However, online platforms are not a homogenous group. This is a diverse sector with each service or platform differing, presenting different opportunities and unique challenges. Indicators of potential harm will therefore differ, with some more important than others depending on the platform, however we believe the focus should predominantly be on the enforcement of terms and conditions; availability of parental controls and development of flagging and reporting systems.

Many platforms' terms and conditions go above and beyond what the law outlines in setting out acceptable standards of content and conduct, allowing users a clear picture of what to expect on the service. In addition, age is not always the best proxy for resilience and it is parents who are best placed, within limits, what is right for their child. Availability of parental controls allow for a more nuanced approach that acknowledges the different speeds of development for children. It is also important that mechanisms are available for users to report harmful content when it is uncovered, and for there to be efficient methods of removal.

When considering harmful content more broadly, or content which may 'impair the physical, mental or moral development' there is often a challenge in defining this content, identifying it and implementing appropriate measures to tackle it.

Where concrete action can be taken with clearly illegal harms, this is not always the case with other more generally harmful content. These terms are less defined, subjective and require a much more tailored response, often needing the context or maturity and resilience of the user to be taken into consideration.

Core to this challenge is the subjective nature of these harms and balancing conflicting rights and responsibilities, including the protection of free expression. When considering types of content which may impair the development of children it is critical that there is a clear, predictable and measurable definition, with a strong evidence base for any negative relationship before action is recommended to be taken.

- **Question 26: How might Ofcom best support VSPs to continue to innovate to keep users safe?**

There are many ways in which Ofcom can best support VSPs to continue to innovate and keep their users safe.

Key amongst these is providing VSPs with the freedom and flexibility in how to achieve their obligations. Creating a clear picture of success and how this can be achieved will be critical, taking into account the characteristics of individual platforms and work closely with them to ensure regulation does not damage their businesses.

Requiring specific mechanisms to identify and remove content, for example user reporting, is not desirable and may not provide the flexibility to deal with content in the most efficient way. Similarly, specific requirements over takedown times for content without taking into consideration how widespread the content in question is may not enable the most harmful content to be prioritised.

In the case of mandated requirements around user reports for example there that they are a far less effective route for some companies to identify and remove content in a timely manner. This would primarily be true in situations where algorithmic processes to detect harm are far more efficient and effective in accurately and quickly identifying harm. Placing undue emphasis on user reporting for companies and harms where effective alternative methods are available could either risk diluting efforts to tackle the harm.

We should also be careful not to commit companies to efforts that would not be directly or wholly relevant to them and the way in which their service operates, which could take away valuable resource from the frontline or more effective action through other platform measures or collaboration forums. It is also important not only to look at what companies are doing here in the UK, for example partnerships with the Internet Watch Foundation, but what international partnerships and collaborations have been undertaken, such as with NCMEC in the USA.

Consideration should also be given to the role of self and co-regulatory approaches which can be more scalable, affordable and effective than traditional regulatory responses. For example, the EU Code of Conduct on countering illegal hate speech has seen enormous progress. The fifth report into the Code of Conduct found that 90% of notifications are now reviewed within 24 hours, with 71% of content removed. This is up from 40% reviewed within 24 hours in December 2016, and 28% of content removed.

In this space Ofcom's most useful role would be that of a trusted forum and convener, sharing best practice, tools and expertise on emerging harms to industry, while taking a proportionate approach that acknowledges that not all will be able to achieve these best practice standards.

In addition, with these new regulations there will be a need for greater expertise and skills to manage new responsibilities, particularly with regards to technology. Ensuring that the proper resources are in place for the challenge ahead will be crucial to helping companies innovate.

Proportionality and Rights

- **Question 23: What challenges might VSP providers face in the practical and proportionate adoption of measures that Ofcom should be aware of?**

The VSP regulation comes at a time when there is a great deal of activity in the digital space at both a national and international level, including specifically for VSPs. Many of these regulatory initiatives are not fully bedded in. From GDPR to the Platform to Business Regulation, Online Harms and the Age Appropriate Design Code, our future relationship with the European Union or DCMS' ongoing review of online advertising, there are a host of new, yet to be implemented or still to be discussed pieces of regulation on the table.

The amount of regulation would create challenges for any business, and it is no different for VSPs. It is not guaranteed that all companies, especially smaller and mid-sized players, have the same resources available to balance these conflicting demands. There is a threat that this work is happening on different timelines with no obvious coordination or assessment of the cumulative impact the recommendations flowing from these pieces of work will have on the ability of companies to achieve best practice or themselves take a proportionate approach that fully takes into accounts the various rights under consideration.

The Digital Regulation Cooperation Forum of which Ofcom is a part is a welcome development, and a step in the right direction towards tackling this issue but more must be done.

These challenges are multiplied if a differentiated, proportionate approach is not taken to specific technologies or reporting requirements.

For example, creating obligations for increased transparency reporting for all VSPs may not be appropriate. Not only do we believe that it would be misguided to attempt to find comparable data-points across all platforms and services due to their diversity, but many of the more established companies have published global transparency reports for many years and are able to commit greater resource to their production.

As such the value of the data collection and analysis will be far greater than newer companies will be able to provide, and the costs of doing so much lower. Creating obligations to report or share data that is not currently collected by a platform or service would also incur significant cost for potentially little benefit. This same principle also applies to the deployment of AI moderation systems.

The introduction of de minimis requirements for low risk services could offer a potential mechanism for adopting a proportionate approach. Based on a risk based approach set out in the GDPR, an exclusion could consider frequency and gravity of previously identified harms on the service (or similar services); size of user base for service; nature of user base for service (e.g. consumers, professionals, academics, parents); type of content on service and potential speed of spread of content based on typical user interaction patterns.

As companies will change and grow over time, any application for exclusion would need to be repeated at regular intervals that reflect whether the fundamentals of the business have changed, in such a way that means the risk of harm has also changed.

- **Question 24: How should VSPs balance their users' rights to freedom of expression, and what metrics should they use to monitor this? What role do you see for a regulator?**
- **Question 28: Do you have any views on the set of principles set out in paragraph 2.49 (protection and assurance, freedom of expression, adaptability over time, transparency, robust enforcement, independence and proportionality), and balancing the tensions that may sometimes occur between them?**

The protection of users' rights to freedom of expression is core to the approach of many VSPs. However, as highlighted earlier in our response, when faced with a range of regulation and limited resource, with potential fines of 5% of qualifying revenue for failure, companies may decide to err on the side of caution and remove potentially harmful content which they would have otherwise been able to give more consideration to. This could potentially lead to over-enforcement and the stifling of legitimate speech.

Here the signal the regulator sends out will be crucial to setting the right incentives. Emphasising a philosophy of best efforts and continuous improvement, with sanctions seen as a last resort, will create the right incentives for companies to consider fully consider borderline content and for freedom of expression to flourish.

This approach would also provide the flexibility for situations such as COVID-19, where there has been a need for greater reliance on machine learning to tackle troublesome content, despite the reduced accuracy compared to a human and machine joint approach.

Adherence and Enforcement

- **Question 25: How should VSPs provide for an out of court redress mechanism for the impartial settlement of disputes between users and VSP providers? (see paragraph 2.32 and article 28(b)(7) in annex 5).**

In considering an out of court redress mechanism, the regulator must take into account that many VSPs receive requests and appeals that are overly-broad, incomplete or made in bad faith. Not all user reporting is reliable or actionable, with recent evidence from YouTube's NetzDG reporting finding over 20,000 incomplete complaints between January and June 2020.

In addition, content moderation is a zero-sum game, with one party getting their desired outcome and the other not, raising the prospect of disputes on either end. In addition, with no friction to lodging a dispute, but requirements to provide out of court redress, systems could quickly become overwhelmed causing a diversion from addressing other, more valid disputes.

- **Question 27: How can Ofcom best support businesses to comply with the new requirements?**

The proportionate, iterative, innovative and agile regulatory approach set out by Ofcom is the right one to take. This should be grounded in constant industry engagement both with those directly under the regulation, but also those whose lead DPA may be in another country.

This engagement will be crucial in the development of guidance, including in setting out the exact definitions of VSPs and the companies in scope. Producing forward guidance, for example how the regulation will blend into the new online harms regime, and what provisions will remain under AVMS after that, will also be helpful.

A high threshold for enforcement or intervention, as seen in other markets such as telecoms, will also be important to enabling businesses to comply with these new requirements. The focus of the regulator should be a collaborative approach with industry that helps to change practices and behaviours so businesses are complaint, with fines or other sanctions seen as a last resort.

This action should not be triggered by individual instances which may be brought up by new and unforeseen challenges, but solely as the consequence of repeated failures of systems and processes over a period of time.