techUK—written evidence (FEO0062)

House of Lords Communications and Digital Committee inquiry into Freedom of Expression Online

Introduction

techUK welcomes the opportunity to provide evidence to the House of Lords Inquiry into freedom of expression online (the Inquiry). Representing the views of the tech sector in all its diversity, techUK has been fully engaged in the debates surrounding freedom of expression, including those relating to regulating online harms and free speech.

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.

techUK is pleased to see that this consultation embodies broader questions regarding online harms regulation, in particular the reference to 'lawful but harmful' online content. Recent events in Washington DC have crystalised different and complex issues which are at the heart of the online harms debate. The divide in public discourse around free speech is not a new phenomenon, yet these events mark a greater need to form an effective and proportionate regulatory framework – one which provides clear definitions of harm and guidance for companies on when they should act to remove harmful but legal content.

Our members remain committed to keeping users safe online and working constructively with Government to achieve a regulatory outcome that is workable and effective in order to protect and empower users, while defending freedom of expression and maintaining the UK's reputation as a pro-innovation and investment destination.

Executive Summary

Freedom of expression is a universal but not unqualified human right protected in international and domestic law as proscribed in Article 19 of the International Covenant on Civil and Political Rights, which the UK ratified in 1976. Over recent years online platforms and services have evolved and presented new opportunities for individuals globally to exercise their rights, with, as summarised by UNESCO, freedom of expression on the internet contributing to "global development, democracy and dialogue".[1]

Opportunities for individual free speech online have also presented some global challenges for governments, communities, and businesses. The subjective

---

[1]   https://en.unesco.org/themes/freedom-expression-internet

nature of individual experiences and perceptions of harm have created a paradox. One individual's free expression online can create an environment where another individual does not feel like they can express freely due to a potential risk or harm. In addition, individuals express themselves online in different contexts for different purposes and drawing distinctions between types of online content is critical to protect free speech. Governments are grappling with this across the world and as we are seeing, regulation of online content is complex.

If we take the UK Online Harms White Paper approach as an example, on the one hand, the proposed regulatory body is intervening and limiting individual free speech which can be offensive and harmful but is still legal, while on the other hand, the same regulator is looking to support existing laws to combat serious illegal content, such as terrorist content or child sexual abuse material (CSAM). While systems and processes are already in place to tackle illegal content, the approach towards legal but harmful content is riddled with intricacies of when free speech online becomes harmful and who should be responsible for deciding what constitutes harm and when a company should act. Given the subjectivity of individual experience and divides in public discourse, we should acknowledge that there are going to be trade-offs in any legal framework which includes harmful but legal content.

What is important is how we deal with these trade-offs considering the context in which individuals express themselves and the associated risks which may result, while ensuring that an evidence-led approach to defining and identifying risk of harm is adhered to.

Technology companies are aware of these challenges and are committed to working with governments to find effective solutions. Digital technologies bring enormous benefits to societies as people rely on digital connectivity not only for accessing information and free expression but also for remote working, socialising, and healthcare, and we should continue working together to ensure that these benefits are not disproportionately impacted by regulation.

In this submission, techUK will highlight the ways in which individuals express themselves online, focusing on collaborative efforts taken by industry, government and society to respond to associated risks on different services.

Our response will advocate for context over censorship, while considering the importance of clear legal definitions and boundaries for harmful but not legal content and pragmatic solutions, such as increased media literacy and education. The questions asked in the consultation will be encompassed in the following sections:

1. Global Freedom of Expression Online

2. Legal & Regulatory Framework

3. Education, Media Literacy and Digital Citizenship

Section 1: Global Freedom of Expression Online

1.1   Global Freedom of Expression Online – the need for context

The context and ways in which individuals express themselves online is diverse and nuanced. On any one day there are 700,000 hours of video uploaded to YouTube, 350 million photos uploaded to Facebook, 500 million new tweets added, and 65 billion WhatsApp's sent. At the same time, users and customers exercise their rights to free speech and equal access to information by, yet not limited to, commenting on online sales websites, leaving online reviews, reading eBooks and journals, accessing news websites and starting petitions.

When individuals sign up to platforms and services online and exercise their right to free expression they are agreeing to the unique terms and conditions and community guidelines of the platform or service which they are using. Terms and conditions are the bedrock for private companies to moderate what takes place on their service, going above and beyond the law. These community guidelines vary from company-to-company and are used to reduce the possibility for harm to occur, depending on the community and environment which the platform or service is designed for.

These standards often include safeguards for scenarios where an individual may abuse the conditions and undermine the service, which usually results in the removal of content and blocking. They act as an incentive for not allowing harm by encouraging violative users to change their behaviour in order to still benefit from the service. It is not in the interests of technology companies to have illegal or harmful content on their sites and collaborative efforts are being made to combat this.

Tackling violative content and illegal crime on platforms, such as CSAM and terrorist content, is often the priority for companies and outcomes are effective. Companies are investing in state-of-the-art AI systems, processes, and teams, as well as working with groups, such as IWF, NMEC, WePROTECT and GIFCT, to rapidly tackle illegal and harmful content on their platforms.

Results can be seen in a recent IWF report, which shows that the UK hosts just 0.04% of global known child sexual abuse URLS, down from 18% in 1996, with the vast majority of this being pushed off the front page of the internet, with search, video channels and social networks accounting for less than 1% of abuse material. In addition, Facebook content moderators have taken down 99.5% of terrorist related posts before they were flagged by users, as identified from their transparency reports.[2] And, for illegal and violative content, the latest transparency report from TikTok shows that 96.4% of videos which breached their community guidelines or terms of service were found and removed by content moderators, 90% of which were before they had received any views.[3]

Companies are also taking steps to combat 'harmful but legal content' online, such as misinformation. For example, Adobe has created a 'Content Authenticity Initiative', building a system to give creators a tool to claim authorship and

---

[2]   https://transparency.facebook.com/community-standards-enforcement
[3]   https://www.tiktok.com/safety/resources/transparency-report-2020-1?lang=en

empowering customers to evaluate if what they are seeing is trustworthy.[4] Google has introduced a new feature on search for information on vaccines, including factual accounts of whether a vaccine is authorised.[5] Meanwhile, TikTok has launched its Covid-19 hub, which has had 14 million views in the UK so far and ensures that all users searching for Covid-19 are directed to verified sources of information and myth busting facts on the virus.[6] And, recently social media companies have agreed a package of measures with the UK government building on efforts to tackle misinformation.[7]

1.2   Global Freedom of Expression Online - responding to the challenge

It is important to look at what is currently being done to respond to some of the legal, ethical, and technical challenges of harmful content caused by the abuse of free speech online, before considering how these efforts can be enhanced. Focusing on how regulation can support and enable technology companies would form part of a collaborative approach to tackling some of the challenges that arise. The sector is committed to working with Government to tackle these challenges and achieve desired outcomes. We would like to see Committee consider the ongoing work and shared commitment to support positive online experiences and how we can work collaboratively to achieve this.

Moreover, we would encourage more nuance both when discussing freedom of expression and when referencing 'technology' and 'online platforms' that might be in scope of regulation. This Inquiry is looking at freedom of expression online, not just of social media companies, and the range of different online services and contexts in which individuals express themselves should not be disregarded. Online platforms and digital services are not a homogenous group. It is a diverse sector with each service or platform presenting different opportunities for individuals to express themselves and access information online, as well as unique challenges. A risk based, proportionate and targeted approach must be taken when attempting to create any overarching framework to tackle these challenges.

In the recent Government response to the Online Harms White Paper, the exemption of some media, including journalism, rightly acknowledges that individuals access information and express themselves in different contexts on a variety of online services, and the importance of upholding media freedom. There are some disparities about which services are excluded and how this links to evidence of risk of harm, with some customer reviews remaining in scope while potentially harmful below the line comments on news sites are exempt. However, the essence of the exemption is a step in the right direction. In theory, it should serve to protect constructive dialogue in a democratic society which is often sparked from authors writing factual accounts of historical events and although could be considered harmful, individuals have a right to access in this context. If this online content were to be caught by this regulation, removed, or censored it would pose a real risk not only to freedom of expression but to

---

[4]   https://blog.adobe.com/en/publish/2019/11/04/content-authenticity-initiative.html#gs.q4rrn5

[5]   https://blog.google/technology/health/accurate-timely-information-covid-19-vaccines/

[6]   https://committees.parliament.uk/writtenevidence/5174/pdf/

[7]   https://www.gov.uk/government/news/social-media-giants-agree-package-of-measures-with-uk-government-to-tackle-vaccine-disinformation

individuals rights to equality, and impact the creative freedom and richness of the UK publishing and literary sectors (the UK is currently the largest exporter of books in the world), and could create online environments which prioritise the voice of some over others.

The recent Government online harms response also outlines a differentiated approach towards companies with some exemptions for 'low risk services'. Despite this provision, the estimated scope still goes far beyond the traditional social media companies in many people's minds and online services of all types and sizes will be required to comply – ranging from services such as TripAdvisor to discussion forums including Mumsnet.

We ask the Committee to consider the variety of different platforms, services and companies that enable free expression online, and the interchangeable levels of risk based on individual use and experience.

1:3   Global Freedom of Expression Online – online content and competition

One of the questions in this consultation groups together online content and competition, asking whether strengthening competition regulation of dominant online platforms would support content moderation. Melding together different policy issues can be problematic, especially when there is limited clarity and a potential for unintended outcomes. There is a need for greater nuance and targeting of policy to avoid putting the wider digital ecosystem into the same basket, and as we address throughout this response, there are evidence-base methods to deal with illegal and harmful content online.

Furthermore, in the Government's recent response to the CMA's Market Study into online platforms and digital advertising, there is mention of how action is being taken on the new Digital Strategy to "ensure coherence of approach, including streamlining the digital regulatory landscape, minimising overlaps and ensuring strong coordination between regulators".[8]

techUK supports the Government's ambition in the Digital Strategy and is looking forward to continued harmonisation of approach, especially when thinking about the different policy areas which are due to land shortly, such as online harms and competition. As the Government has not yet outlined what UK competition regulation means for companies, the reference and link to implications on content moderation feels out of place in this Inquiry. It may well be that some link could be made between the two policy objectives, but without clarity from the Government on competition and online harms, this question encourages speculation which might not be conducive to evidence based, coherent policymaking. In sum, the Inquiry should consider how competition issues need to be dealt with in a competition law context and dealt with first, before looking for links to online harms.

---

[8]   https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study

Section 2: Legal & Regulatory Framework

2.1   Legal & Regulatory Framework - regulating global free expression online

The exercise of freedom of expression online sits within existing domestic and international legal and regulatory frameworks, protecting individuals from some of the most serious crimes online. In many countries across the world, criminal legal systems are in already in place to combat illegal activity online. To take the UK as an example the Law Commission found in their review of abusive and offensive online communications, that it can be the case that they are criminalised online to a same or even a greater degree than the equivalent offline offending. The Law Commission found challenges not with the legality of online content, but with the number of overlapping offensives and ambiguous terms such as 'indecency' and 'gross offensiveness' causing confusion. As we will outline in this response, forming legal definitions and terms is at the crux of the challenge when thinking about online harms regulation and freedom of expression, especially when harmful but legal activity is to be included in scope. Any new framework will need to be robustly enforced, ensuring that the police have the capacity and capabilities to do so.

Furthermore, for online harms, it is often advertised that regulatory systems are of technology companies, when instead they are regulating individual behaviour with technology companies acting as the enabler. Online harms regulation has the potential to intersect individual experiences, opinions, and rights online, and collaborative efforts should be made to ensure that the regulatory outcome is proportionate – both to preventing harm and protecting the range of online services which society so heavily relies on.

Best practice legal examples include the E-Commerce Directive and principle of limited liability for online intermediary activities, which have set a long-standing foundational legal framework that underpins the internet and has been fundamental in supporting expression online and growing Europe's digital economy. They have allowed a diversity of intermediaries and services to develop, become established and grow, while also providing previously unimaginable opportunities for people and businesses to access new markets while safeguarding the important right to free online expression. The existing legal framework also provides an important and implicit link between the role a platform plays and the content it hosts, with increasing involvement leading to increased liability and vice versa.

We have seen the unintended consequences of strictly enforced regulation - such as fines and criminal liability - play out in Germany. Technology companies have no doubt acted cautiously under NetzDG by removing infringing content to avoid possible sanctions, which has led to satire material being incorrectly removed. A number of organisations have already been vocal in their concerns - Big Brother Watch, Article 19, the Open Rights Group and Index on Censorship for example signed a joint letter[9] highlighting censorship concerns. To avoid censorship becoming the norm in free societies, equal focus should be given to moderation and the role of individual behaviour. While companies need to ensure that their

---

[9]   https://www.theguardian.com/world/2019/apr/10/internet-regulation-proposals-could-censor-the-lawful-speech-of-millions

platforms are safe, citizens also need to be educated to develop better digital rights which prevent them from violating terms of service.

Strict enforcement measures have the potential to create a slippery slope for companies removing content and could result in unintended consequences for the individual exercising their rights. To take a potential 'duty of impartiality' as an example from the UK online harms debate - if coupled with strict enforcement - there is a real risk that companies may have little choice but to restrict legitimate expression of political views, undermining not only human rights but also the democratic society which we live in.

As highlighted in the Executive Summary, freedom of expression is a derogable human right in both UK domestic and international law. The UK should ensure that any regulatory framework being developed is fully aligned with the UK's obligations as a signatory to the ICCPR and, as the UN Special Rapporteur on freedom of expression urged, "refrain from adopting models of [online content] regulation where government agencies, rather than judicial authorities, become the arbiters of lawful expression. [And] avoid delegating responsibility to companies as adjudicators of content, which empowers corporate judgment over human rights values to the detriment of users".[10]

techUK believes that the UK has a unique opportunity to take stock of the international policy environment and ensure that any new regulatory system meets the highest international standards in order to limit the ability of less-democratic states to use the UK's approach as a green-light for more draconian measures.

2.2   Legal & Regulatory Framework - scope of companies

To help companies better understand their obligations, further clarity is needed on where the legal boundaries of free speech are drawn and how this might impact the scope of regulation. Our members offer a range of different services for individuals to exercise their rights online, and depending on how individuals use their platforms, there are varied levels of possible risk or harm.

Each harm exists in different ways on different services (and none on others) and presents a different and unique challenge for the application of technology, with the clearest success seen in harms that are clearly definable, such as copyrighted material or CSE content. Furthermore, to add to the complexity, some platforms are used for educational, social, and professional purposes, and it is unclear where the legal boundaries would lie for individuals expressing themselves. Content creators who are writing historical accounts of events which might be viewed as harmful fall into a grey area, as well as publishers on online marketplaces.

To our earlier point regarding the need for nuance when talking about 'technology', the Inquiry should consider how a detailed and balanced regulatory approach is needed when thinking about the variety of companies in scope, their different functionalities and potential lack of accessibility to tools, skills and resources.

---

[10]   https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/ContentRegulation.aspx

techUK believes the regulator should designate companies in scope, as proposed in Ireland's Online Harms regulation. This would represent an important step in supporting proportionality for companies, ensuring that those with limited consumer interaction are not in scope.

2.3   Legal & Regulatory Framework - defining harmful but legal content

As outlined above, there are existing UK laws in place to combat illegal activity online and while it is appropriate that illegal content and legal but harmful content are treated differently, the Inquiry must consider the toughest questions that would assist companies in the identification and removal of harmful content, primarily the definition of harm.

Who defines harmful content is a key aspect of any upcoming regulatory regime, and it is important that there are strong democratic safeguards in place so that legal content offline is not made *de facto* illegal online. It is critical that when it comes to *legal* content, companies should only be required to enforce their own terms and conditions, to fulfil the Government's commitment to protect users' rights online and not "prevent adults from accessing or posting legal content, nor require companies to remove specific pieces of legal content".[11]

When asking questions around whether 'online platforms [should be] under a legal duty to protect freedom of expression', we would advise the Inquiry to consider what this will look like in practice, especially for smaller companies with less resource. From our experience in online harms debates around 'duty of care' and a rumoured 'duty of impartiality', there is sometimes confusion within the sector about what is practically required from different companies to comply, with stakeholders taking subjective judgements on what these duties might mean.

Unless clearly defined, a 'legal duty to protect freedom of expression' has the potential to add to this confusion by feeling abstract and unrelatable. It could also place too much responsibility on the sector to decide what constitutes free speech and where the line is crossed to result in harmful content. It is often difficult to define when someone is being ironic or has malicious intent; whether someone is spreading disinformation or is just misinformed; or whether someone is trolling or simply teasing a friend. With this in mind and given the proposed regulator in the online harms regime could also have a duty to look at protecting freedom of expression, it is not clear what the benefits would be of companies having this duty. There is an additional risk that - if coupled with strong liability measures - it could have unintended consequences on Article 19, as we have outlined above in relation to the 'duty of impartiality'.

Requiring private companies to define these issues and boundaries alone and proposing significant sanctions when the wrong decision is reached could have significant adverse outcomes. By contrast, clear definitions and legal boundaries would give industry the confidence to act without making their own moral or political distinctions on content, enabling them to act more quickly and decisively, rapidly improving their ability to tackle harmful content. In addition,

---

[11]   https://www.gov.uk/government/consultations/online-harms-white-paper/public-feedback/online-harms-white-paper-initial-consultation-response

empowering individuals to have the confidence on how to act online without perpetrating will enable positive user experiences.

techUK believes that the focus of regulation should be on where the most value can be added: defining harms, providing clarity where there is uncertainty and adjudicating where boundaries lie. This would allow for a more targeted and effective approach.

2.4   Legal & Regulatory Framework - transparency and algorithms

The Inquiry asks about the role of transparency and algorithms, including whether regulators should play a role. When addressing this question, it is important for the Inquiry to look into the ways in which individuals express themselves and how this can result in harmful content online, as well as existing efforts from the sector to improve transparency and content moderation. Transparency can help users to feel safe online by building trust in services, and companies are already putting in efforts to support this. For example, TikTok has set up a 'Transparency and Accountability Centre' providing users the opportunities to review how content moderators apply Community Guidelines to review the content and accounts which are escalated to them via user reports and transparency-based flagging. It also gives users the opportunity to understand how the applications algorithm operates.[12]

Trust, transparency and accountability are incredibly important. However, when operationalising into a regulatory framework, there is a need to be very clear about the meaning and purpose of these terms and consider the desired outcomes for different audiences. For example, creating obligations for increased transparency reporting may not lead to the best outcomes, particularly if this is intended to be made public rather than kept private.

Additionally, 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. Creating obligations to report or share data that is not currently collected by a platform or service would also incur significant cost for little benefit. Rather, we believe the priority is to provide users with information that is useful for them to understand the issues in meaningful and innovative ways.

We believe this differentiated approach based on harm and risk is best developed by the company who are best placed to communicate with their users, which would provide meaningful and useful transparency. In the Government's recent full response to the Online Harms White Paper, the majority of companies will not be required to conduct mandatory transparency report and for the reasons we have listed above, it is important that this provision remains as we move through the 'Online Safety Bill' legislative process.

---

[12]   https://www.tiktok.com/transparency?lang=en

Section 3: Education, Media Literacy and Digital Citizenship

3.1   Education, Media Literacy and Digital Citizenship – empowering users

Education and empowerment should rightly be a focus of the Inquiry. Balancing competing individual rights and regulating content online remain very human issues and we should not lose sight of the fact that we are not discussing regulation of companies who host user generated content but the regulation of individuals and what they say and do online.

Digital literacy must be a greater priority and focus in on changing behaviours over time and instilling 'digital civility'. It is vital that we empower and educate users of all ages to navigate the online world safely and securely.

Education can play an important role in helping society develop digital behaviours and skills online, enabling kinder and more equal individual experiences. Companies already either create their own tools to help empower and educate – whether for children, their parents, teachers or vulnerable adults, or partner with other providers to do this.

It is vital that regulation does not cut across this work, but instead builds on it to ensure there is a concerted effort to create an inclusive strategy that responds to the varying needs of users. The Government or proposed regulator should act as a convenor for the relevant stakeholders to come together and share information, best practice, and offer a place to co-ordinate action.

3.2   Education, Media Literacy and Digital Citizenship - anonymity and pseudonymity

There has been some suggestion that removing anonymity – or allowing pseudonymity with companies made to verify the identity of their users – would be one solution to limiting the spread of misinformation or abuse. There are significant questions over the efficacy, appropriateness, or desirability of such a move, which could create significant unintended consequences, including the potential for data leaks.

People sharing misinformation online are often doing so with their real identity, sharing not out of malice but misguided concern. Removing anonymity would not change this behaviour but would impact the many legitimate uses of anonymity online. These are people who use anonymity for the safety and security it provides them to live their lives – from journalists and whistle-blowers to ordinary people for who anonymity gives them the confidence to seek help, information and advice on sensitive issues such as abortion, mental health or sexuality. The lives of people in politics and media are somewhat atypical to the people they represent, and the Inquiry consider the various groups of individuals who may be at risk if they are not allowed to be anonymous online.

There are multiple examples for why anonymity and pseudonymity are essential for individuals to effectively exercise their rights under Article 19 of the ICCPR. To name a few - if you work in the public sector, such as for the police or NHS where there are rules about expressing views, anonymity might be the only way which you can legitimately share your thoughts and political opinions online. This

is also the case for experts who may not be able to comment under their real name due to potential reputational or confidentiality, and for children who might not feel comfortable seeking support online if they have to give their real name. We can see cases of anonymity and pseudonymity playing out in the real world, for example where books are written under pseudonyms to protect the professional author from scrutiny, and we should not have a different standard online.

Moreover, it is often assumed there would be no downside to requiring people to register with their identity on online services, however this could have a significant chilling effect. Recent years have seen a number of database breaches that highlight how people's information can be leaked. Given that this Inquiry is focusing on freedom of expression *online* not just for *social media,* there is a need to look at the broader range of services which individuals might have to sign up their identity to, and whether society would be comfortable with this.

While for some this may not be a concern, having their personal identity connected to their online persona could have a drastic and irreversible impact for others – from the domestic abuse victim seeking advice to an individual being outed in a community for their personal, political or religious views.

Furthermore, it is important to consider the effectiveness of UK citizens verifying their identity online, and whether abusive and offensive content will be reduced. If verification of identity is to only impact people in the UK, there is a possibility of creating an uneven playing field for businesses when creating new services. It also has the possibility to create opportunities for people in the UK to be subject to further abuse, especially if they have to disclose their identity to online offenders. Finally, it would do nothing to stop the most determined bad actors, who will find ways to get around the system to hide their identity and continue their abuse. Meanwhile, the majority of individuals who might use anonymity for legitimate reasons would be prevented from this function, resulting in a contradictory outcome.

15 January 2021