# Written evidence submitted by techUK (COR0179)

## About techUK & COVID-19

1. techUK welcomes the opportunity to provide evidence to the Home Affairs Committee Inquiry into preparedness for COVID-19. techUK represents over 850 technology firms from large multinationals that are major investors and employers in the UK to small, innovative domestic companies that are working hard to scale up.

2. The tech sector has mobilised quickly to support the frontline fight against COVID-19, working to support the Government, the NHS, businesses and individuals respond and adapt. Industry continues working with multiple Government departments to ensure **digital resilience and continued connectivity** through the crisis, managing unprecedented pressure on their products and services so that people can continue to communicate, entertain and remote work.

3. Thousands of devices from companies such as **Facebook** and **Samsung** have been distributed to NHS workers, children and vulnerable people who would otherwise be digital excluded, and Internet Service Providers have published a package of support for the NHS including additional mobile data, voice calls and texts for NHS frontline staff and broadband upgrades for care homes and clinicians working from home.

4. Meanwhile, ground-breaking partnerships have been activated between Government and industry, with **Google** and **Microsoft** among others providing services and support to schools for free to support **online learning** and helping to set up online **digital skills training** for people who have been furloughed or lost their jobs.

5. In addition, since the outbreak of the virus data has quickly become a vital tool in the race to mitigate the spread of the virus and protect the public. **Google**, **Facebook** and **Apple** have each produced mobility data trends and Disease Prevention Maps to inform disease forecasting efforts and protective measures enacted by Government. At the same time, companies have worked collaboratively with Government, healthcare organisations and other stakeholders to tackle misinformation, promoting verified sources to users.

## Executive Summary

6. In this submission techUK will focus on the Online Harms element of the Committee's inquiry, considering their adequacy to address issues previously identified or arising from the pandemic, and their pitfalls. techUK has been fully engaged in the Online Harms process with the Home Office and DCMS, representing the views of the tech sector in all its diversity.

7. Digital technologies are used every day and bring enormous positive benefits to people's lives, particularly at the moment as people rely on digital connectivity for remote working, socialising and accessing healthcare and information. These benefits are the result of a public policy environment developed through the years that promotes innovation and embraces technological change.

8. In these extraordinary times we have seen unprecedented action as industry is meeting both vastly increased demand for the products and services with new challenges brought about by rapidly changing usage patterns, all the while facing the same challenges facing most other businesses across the economy.

9. techUK is pleased to see continued progress being made by Government on the issue of online harms. Our members remain committed to keeping users safe online and working constructively with Government to achieve an outcome that is both effective and proportionate. One that protects and empowers users whilst maintaining fundamental rights and the UK's reputation is pro-innovation and investment nation.

10. techUK supports the Government's approach in the Online Harms debate – one which focuses on systems and processes rather than attempting to adjudicate individual pieces of user content, and their commitment to a risk-based and proportionate approach.

11. However, significant questions and challenges remain following the publication of the initial consultation response, pre-legislative scrutiny is both necessary and desirable.

12. Primarily these outstanding questions and challenges focus on:

1) The scope of online harms under consideration
2) The businesses in scope of regulation
3) Details on the regulatory framework
4) Education, media and digital literacy

## Scope of Online Harms

13. The Online Harms regulation seeks to address a variety of different harms ranging from the clearly illegal to those which are lawful but potentially harmful or harmful to a specific group (whether young people or those with other vulnerabilities). In seeking to address such a broad spectrum of harm within same regulatory approach techUK believes nuance and proportionality is at risk of being lost.

14. Different policy responses are necessary for different harms – for example, terrorist material is already illegal and therefore is, and should continue to be, acted on quickly with a zero-tolerance approach. There are clearly established and tested methods to tackle this content, both domestically (through the Counter-Terrorism Internet Referral Unit) and internationally (via the Global Internet Forum to Counter Terrorism). Meanwhile, issues such as coercive behaviour (a harm identified in the White Paper as 'harm with a less clear definition') do not have such existing frameworks and may require a more sensitive approach to determine the extent of the harm and appropriate action required – taking into consideration wider contextual issues that may not be apparent at first glance.

15. techUK is unclear what benefits would result by treating such a wide-spectrum of harm under one framework and believe the risks outweigh any marginal gains. We welcome the work underway to identify overlap between harms in the White Paper and other existing or planned regulatory frameworks, and deference should be given to the latter.

**16. techUK believes that there needs to be a clear separation in the way that 'illegal content' and 'legal but harmful' content is tackled in the Online Harms framework. Attempting to tackle both risks creating too broad a regime which may overwhelm the regulator or lead to unintended consequences, such a greater regulation of speech online than offline.**

### *Scope of Online Harms – the Definition of Harm*

17. While it is appropriate that illegal content and legal but harmful content are treated differently, the proposed regulation still avoids the toughest questions that would assist companies in the identification and removal of harmful content, primarily the definition of harm.

18. Who defines harmful content will be 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, in order 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".

19. By leaving the decision to industry a core challenge in tackling harmful content is ignored. 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 is simply teasing a friend. Requiring private companies to define these issues and boundaries alone, and proposing significant sanctions when the wrong decision is reached could have significant unintended consequences.

20. By providing clear definitions and legal boundaries industry would be given 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.

**21. techUK believes that the Government and future regulator should focus 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.**

*Scope of Online Harms – Establishing the Evidence Base*

22. The Government has provided many examples of harms it wants companies to tackle and acknowledges that the lists provided are neither "exhaustive nor fixed".

23. We understand the desire not to be too prescriptive in listing harms for fear that a "static list could prevent swift regulatory action to address new forms of online harms, new technologies content and new online activities". However it is important that any harms companies are expected to act against are based solely on the basis of evidence.

24. techUK would advocate a programme of work from the new regulator that tracks the types of harms developing and makes recommendations on further action.

25. In keeping with a risked-based approach techUK would advocate the works with industry, academics and other experts to track and build the evidence-based of emerging harms to ensure that action is taken in a targeted and proportionate manner, responding to risks as they exist. This would help prevent kneejerk reactions, as seen around the 'Momo Challenge' hoax which saw parliamentarians, police, schools and the public around the world call for action despite the harm not existing.

26.We also believe there is a role for any new regulator to commission their own independent research of the general population and undertake in-depth studies to produce reports such as Ofcom's *Connected Nations* and *Online Nation.* These reports have become vital in the toolkit of interested consumers, parliamentarians and other stakeholders helping to educate, inform and raise awareness of key issues.

**27. techUK would recommend that Government takes a more staggered approach that deals with those harms with a strong evidence base first while building an evidence base on issues where there is less consensus and a lack of evidence. This should be done through the commissioning of independent research and consultation with a wide range of stakeholders.**

**28. This approach would have the benefit of enabling action with certainty where there is a strong evidence base and allow for agile responses as harms change or new harms surface.**

## Businesses in Scope

29. The scope of the Online Harms regulation has been drawn very broadly, encompassing any service that "allow users to share or discover user-generated content or interact with each other online".

30. This means that online services of all types and sizes will be required to comply – from Argos' retail website (which allows users to post reviews of their purchases) to TripAdvisor and even discussion forums such as Mumsnet. With such a broad scope, it is even more important that proportionality and a risk-based approach is at the heart of the regulatory regime.

31. While the Government most recently estimated that the regulation proposed would only effect 5% of UK businesses this still accounts for approximately 300,000 UK businesses, far beyond the traditional social media companies in many people's minds when this issue is discussed.

32. As the economy digitizes this scope will only grow, as more and more businesses create an online presence that may facilitate user-generated content, presenting a greater and greater challenge to the regulator. While enforcement will no doubt be proportionate this will only serve to increase the costs and stress faced by many small businesses.

33. The White Paper is clearly written with social media in mind and the full impact of Online Harms regulation on platforms with a different focus, who do not necessarily host content, is unclear.

**34. The Online Harms regulation should be focused on these social media companies, with the regulator designating those companies in scope, as proposed in Ireland's Online Harms regulation. This would represent an important step in ensuring proportionality for companies, ensuring that those with limited consumer interaction are not in scope.**

**35. techUK would also like to see the Government conduct a full economic impact assessment to better understand the implications of the White Paper and related digital policy on the digital economy when taken together**

*Businesses in Scope – B2B Companies*

36. The Government's announcement that B2B companies will be removed from scope of the regulation, alongside journalistic content is welcome, however the proposed scope of the regulation remains much too wide, and further guidance will be needed on whether some companies are in scope.

37. B2B platforms should be defined according to their intended or targeted user base, to avoid companies suddenly finding themselves in scope of the regulation. For example, COVID-19 has seen a rapid change in how many products and services are used, with some B2B platforms seeing an uptick in consumer use.

38. It would not be appropriate to place the significant burdens under the Online Harms framework on a B2B business for what may amount to a temporary and limited change in their userbase. Requiring these companies to apply the regulations even for the limited number of consumer users would require a much greater level of data collection which could be opposed by their bulk enterprise clients, or could run contrary to the GDPR principle on data minimisation.

*Businesses in Scope - Private Messaging*

39. In addition techUK is worried that proposals appear to suggest that the new regulatory framework would apply to private spaces and believes that private communications should be excluded from any new regulation.

40. Private communication would, for example, include closed groups online that requires an individual to actively join, communication/discussion channels that are employed in businesses to facilitate internal communication functions as well as clearly private communications between small groups whether via email, SMS, or any other service.

41. If the intent is to include private messaging in some capacity the Government should consult expert legal advice, including data protection authorities, to see how such measures would be compatible with GDPR.

## Regulatory Framework

42. It is important to bear in mind that while this is advertised as regulation of technology companies, it is in fact regulating user speech with the company acting as an enforcer.

43. It is right that the regulator must have "an obligation to protect users' rights online, particularly rights to privacy and freedom of expression" and not "prevent adults from accessing or posting legal content, nor require companies to remove specific pieces of legal content". However, we need to be clear about what trade-offs will be created by this new framework.

44. When faced with the choice between fines and possible criminal liability or removing possibly infringing content companies will no doubt act cautiously. We have already seen this happen elsewhere for example in Germany where the NetzDG Act 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 highlighting censorship concerns.

45. There is much work to be done to clarify how regulation will be done in a way that is proportionate, pro-innovation and safeguard users' rights. These concerns are precisely why effective oversight and governance will be critical for any regulator.

**46. With the ability to effectively outlaw types of speech online the regulator will have an unparalleled position in modern Britain. It is only right that Parliament has a central role in providing oversight of this new regime.**

*Regulatory Framework – Ofcom as the Regulator*

47. techUK notes that the Government is minded to name Ofcom as the regulator. Ofcom's experience makes it an appropriate voice in this debate but if it is to take on this new role, vastly expanding on its current remit, it must be given the appropriate resources and be upskilled to meet the challenge ahead.

48. However, not all of Ofcom's lessons from broadcast regulation appropriately translate. The scope of businesses Ofcom would need to deal with would vastly increase under these proposals. Currently, Ofcom regulates a small number of TV and radio stations, which would grow considerably in the current scope of the regulation.

49. Furthermore, broadcast regulation covers a much smaller amount of content, with only 24 hours in a day. In comparison, there are over 500 million tweets a day, 500 hours of content uploaded to YouTube every minute, and billions of people are active on Facebook everyday. This will require a different approach by Ofcom.

50. Such scale also raises a question for the funding of the regulator – Ofcom is currently funded by a fee on all those under its scope, however this would not be appropriate for an online world and would amount to a tax on user-generated content. Careful consideration will need to be given as to how the regulator has the proper resources it needs to do the job well.

*Regulatory Framework – Enforcement*

51. We await details of the enforcement powers that the regulator would have to tackle bad actors. However, we believe the primary emphasis must remain on working to change policies and practices by working in collaboration with companies. We believe that heavy enforcement powers will not be effective against bad actors and the existence of such powers will have unintended consequences for the rest of the market.

52. We were disappointed to see that proposals to impose liability on individual members of senior management remained in the Government' initial consultation response techUK believes this sends the wrong signal to those who might wish to invest in the UK and would be a huge disrupter to the success of the UK tech sector.

53. It would discourage start-ups from choosing the UK as their destination of choice, and discourage new investments at a time when we should be captalising on the sector's record growth and investment. Fines over and above those already in place for GDPR are likely to have a further chilling effect on investment in the UK digital economy.

54. Moreover, increasingly harsh sanctions ignore that these are difficult decisions where the wrong decisions are sometimes made not out of malice or negligence but because of subjective nature of some of the harm.

55. Such sanctions would also be targeted at the good actors in this space, those regularly engaged with Government to come the right decision, rather than the most harmful actors. These are companies in foreign jurisdictions who may have no interest in abiding by any regulation, or nominating a UK director. It is important we look at how enforcement would help tackle these actors, rather than those currently constructively engaging in the process.

**56. techUK is clear that any enforcement powers must be proportionate and fair. Senior management liability, excessive fines or ISP blocking would indicate a move away from this approach.**

Regulatory Framework – Age Verification

57. Beyond deciding what type of legal content or behaviour is acceptable on their services, the Online Harms proposals suggest an further responsibility to take "reasonable steps to protect children from harm" and offer children a higher level of protection.

58. It is unclear if this obligation overrides the ability of companies to decide what content should be allowed on their service, or how it could impact the commitment for Government not to restrict adults' ability to view, share and post legal content.

59. The proposal to rely on age assurance and age verification technology is a worrying development. As we have highlighted in our responses to the ICO's Age Appropriate Design Code, this is an area fraught with challenges. There is a risk that regulation would lead to age verification becoming the norm for most, if not all, services in scope. This could have very significant implications that need to be assessed and thought through carefully.

60. There are real questions about whether the wider use of age verification is in the interests of either the user of a service or the service provider. Implemented badly, this could lead to a situation where companies are encouraged to collect more data, including documentation to verify age and introduce log-in measures to minimise disruption to user experience.

61. Moreover, it is questionable whether robust, privacy centric and user-friendly age-verification tools are sufficiently well developed to be deployed at the scale and pace that would be required for companies to comply. Many companies have no desire to collect highly personal ID that may be used to verify age, such as passports.

62. Not only would this provide high burdens on companies, but could also lead to the restriction of children's access to vital online services, either because they are unable to purchase new forms of ID, or because some only services may opt to make their services only available to adults to reduce the liability under the regulation.

63. The Safer Internet Centre recently published research which showed how critical the internet is to young people's development and identity. We should be wary of any proposals that would restrict this.

## Education, Media and Digital Literacy

64. The recent pandemic has rightly seen a focus on the risks of misinformation and disinformation. Since the start of the crisis we have seen unprecedent action across the board to demote and remove misleading, inaccurate or harmful content, as well as to promote authoritative sources of information from the Government, WHO, NHS and Public Health England. For example, 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.

65. The behaviour and content we see in the online world is a reflection of the offline, and tackling misinformation is a societal challenge rather than a technical one. It is incumbent on us all to promote accurate and insightful information from trusted and official sources while discounting misinformation

wherever it is found, even if shared from a known friend, family member, world-leader or morning TV show host.

66. COVID-19 is just one issue – new challenges will emerge both in public health and in the broader information environment, and each will require a different response. To tackle misinformation in the long term – not just for this crisis but for the future – we need to vastly improve media and digital literacy, alongside technical solutions.

67. If we can improve people's resilience to mis-and-dis-information, instilling critical thinking and helping them spot and promote only information from authoritative sources we can future proof society from similar challenges in the future. This should be at the heart of the new regulator's priorities.

Education, Media and Digital Literacy – Empowering Users

68.Education and empowerment should rightly be a focus of the online harms debate. While we discussing online harms, at their heart these 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 users and what they say and do online.

69. Therefore, 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.

70. While the pandemic has highlighted the problem of digital exclusion, in mere weeks we have seen some ground-breaking and potentially life-changing initiatives launched by both industry and Government, with COVID-19 presenting a unique opportunity to improve the digital experience for people across the country.

71. 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. However, it is harder to reach adults who may lack digital confidence and other vulnerable users.

**72. 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.**

Education, Media and Digital Literacy - Anonymity

73. 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.

74. There are significant questions over the efficacy, appropriateness or desirability of such a move, which could create significant unintended consequences.

75. People sharing misinformation online are often doing so with their real identity, sharing not out of malice but 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.

76. It is often assumed there would be no downside to requiring people 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.

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

78. Furthermore, for those most troublesome cases of people sharing disinformation or abuse, enforcing identity may actual hinder enforcement action. These bad actors are much more likely in this situation to mask their identity online, for example by using a VPN to access the service from a different jurisdiction. This would make it harder for online platforms to continue their work to help law enforcement track, disrupt and prosecute these bad actors.

May 2020