Written evidence submitted by the Internet Association (OSB0132)

Summary

Internet Association ("IA") welcomes the opportunity to respond to the Draft Online Safety Bill (Joint Committee) call for evidence as it continues to consider the Government's draft Bill to establish a new regulatory framework to tackle harmful content online. IA believes that the internet sector needs a balanced policy and regulatory environment to continue, and grow, its contribution to the UK economy, consumers and society in the future.

Internet companies already take significant action to address harms

Internet companies support the broad approach to improving the regulatory environment to ensure the UK is the safest place in the world to be online. And while solving these problems is not easy - with tens of thousands of companies in scope ranging from social media, online forums, online marketplaces and more - as an industry we are committed to reducing harm online. Indeed, what is possible in relation to tackling harm is increasing every month.

Some of the discussion around the release of the Government's Online Safety Bill continues to suggest that harm only persists on the internet because internet companies do not care or are not trying hard enough to tackle it. We fundamentally reject this characterisation – as set out above, internet companies have not waited for legislation and have taken, and will continue to take, significant steps to address harms on their services a. However, it is clear that there is not an easy or one-size-fits-all way for internet companies to instantly eliminate all online harms.

Key concerns with the Online Safety Bill

Duty of Care and senior management criminal liability

A Duty of Care model - which has been used in other areas of law - is much harder to apply for online spaces and will need to be approached with care in its application.

There are good reasons why we do not introduce legal duties of care whenever we have a policy goal. We do not introduce a duty of care for newspapers to ensure that their readers are perfectly informed, or a duty of care around environmental sustainability. While these are important societal goals, the way we have decided to tackle them is with specific regulations setting out very clearly the role of companies.

There are often hard trade-offs between different societal goals such as privacy, safety and innovation – and these need to be actively considered. Any duty of care model should focus on ensuring robust processes and systems are in place.

Indeed, the Lords Communications and Digital Committee's recent report laid out a view which would warrant further thought by the Government as it proceeds: "The duty of care approach should inform a flexible framework for digital regulation, guided by underlying principles, including freedom of expression, which is able to adapt to the rapidly developing digital world while setting clear expectations for platforms."

In relation to this issue is the inclusion of criminal liability for senior managers - though IA notes that this will not be introduced for at least two years after the regime is fully operational and only if services do not 'step up their efforts to improve safety'.

The UK has an ambition to become the safest place to be online - but also the best place to work and start a business in the thriving tech sector. But managerial liability and sanctions of the type held in threat through this Bill has the potential to make the UK less attractive to professional talent that is needed to help the UK's tech sector continue to grow - but also to innovate and find new ways to tackle online harms.

Freedom of Expression

While it is welcome that the Government has included the requirement for safeguards to be put in place to protect freedom of expression - it is likely that the reality will be very different based on the current proposals. And the duties on freedom of expression should be strengthened and given equal weight to the safety duties - with internet companies requiring more clarity about how these duties need to be balanced in practice.

Of particular concern is the independence for the regulator to decide the list of harms. While the initial list of illegal content has a focus on incitement to terrorism or violent extremism - which is already illegal and internet companies strongly agree with rooting out of our platforms - it is not hard to see the creation of a slippery slope as a precedent is created that the state can shut down any speech that it finds objectionable. Already we are seeing pressure to include in scope of the online harm duty of care books that argue for ideas we dislike.

The Government has previously argued that the regulator should "not be responsible for policing truth and accuracy online". In practice, however, it will be hard for this safeguard to have teeth while maintaining the current and continued unspecified definition of legal but harmful content. While platform providers can perform a helpful moderation role, encouraging their audience to consume a variety of viewpoints, there is a significant difference between this and attempting to ban or censor speech.

Scope of services

While the Government explicitly recognises that private communications should be treated differently, it gives little guidance on what this will mean practically - or how 'private' is to be defined. Coming up with a workable definition is likely to be challenging. Many online services already significantly blur the line between public: posts to your Facebook News Feed, for example, may be intended for an audience of friends and family in the hundreds, but still not for the Internet at large. And while Schedule 1 of the bill specifies certain services and content excluded from the scope of this regime - including emails, SMS messages and MMS messages - but the exclusion applies only if the services or content represents "the only user-generated content enabled by the service," so Facebook Messenger, for example, does not qualify and it would be regulated.

The bill also gives significant power to the Government to amend Schedule 1 to add new services to the list of exemptions or remove some of those already exempt. This power gives Ministers a significant level of discretion, which, if misused in the future, could lead to policing private messaging and communications channels. While the main focus here would

likely be illegal content such as terrorist and CSEA content, questions about the effect of the bill on encryption, security and privacy remain unanswered and will be important for the Government to clarify.

Legal but harmful content

The continued approach being taken by the Government surrounding 'legal but harmful' content has significant problems of subjectivity - especially around the definition that such content causes "physical or psychological harm".

Given the enormous scope of activities undertaken on the Internet, the current proposals effectively give the proposed regulator enormous discretion to unanimously outlaw or discourage particular activities or types of speech. An important check and balance in a democracy is that when a society recognises a new problem, new law from Parliament or the courts is debated and argued rather than unilaterally implemented by the executive.

Rather than a one-size-fits-all approach, we need to take each harm individually, and look for a proportionate response. Treating extremist content under the same framework as infinite scrolling pages ('designed addiction') risks criminalising legitimate speech and introducing massively disproportionate intervention.

In order to avoid mission creep, we believe that at minimum the new regulator should be required to provide an updated list of the specific harms it is concerned with and the evidence base lying behind them. A better safeguard still, however, would be for the regulator to be given a specific list of harms to address, which could then be revisited on a recurring basis.

Economic growth and international impact

One particular worry is that in practice, the only way to meet many of the demands of a new duty of care will be through the introduction of mandatory filtering. Beyond the potential impact on free expression, this kind of content filtering can be extremely expensive to develop and iterate - and often needs to be complemented by significant amounts of human moderation.

As well as slowing future innovation, these rules could lead to a worsening of the quality of Internet services consumers already receive. The best way to avoid this chilling effect on innovation is to ensure that any remedies are based around a specific list of harms, with a clear evidence base of harm and a quantified regulatory impact assessment of best practice in reducing risk.

As an organisation with representation in both the US and the UK, IA is well placed to make a judgement on the impact the Bill will have on the UK globally.

The US and UK both have vibrant digital economies and strong commitments to the open internet. One sign of the strong, reciprocal digital trade relationship between our two countries is that both are the most important cross-border e-commerce markets for each other, and both are world leaders in digital exports. The U.S. now exports $48.8 billion (£39 billion) in digital services to the UK, an increase of 52 percent from 2006 to 2018. Similarly, the UK now exports $34.8 billion (£27.8 billion) to the US, an increase of 56 percent from

2006 to 2017. The US and the UK also rank numbers five and six, respectively, among OECD countries for their share of predominantly digitally-delivered services in commercial services trade. And nearly one fifth of each economy's total employment is in ICT task intensive jobs.

It sets a crucial example for other countries to follow. At a time when countries like China, India, and Russia are pushing very different, closed visions of the internet, it is crucial for our two countries to coalesce around best-in-class international digital regulation for the 21st century. Getting this Bill right forms a key part of this.

Internet Association: Joint Committee Submission – Full Submission

1. Introduction

Internet Association ("IA") welcomes the opportunity to respond to the Draft Online Safety Bill (Joint Committee) call for evidence as it continues to consider the Government's draft Bill to establish a new regulatory framework to tackle harmful content online.

IA represents over 40 of the world's leading internet companies and is the only trade association that exclusively represents leading global internet companies on matters of public policy. IA's mission is to foster innovation, promote economic growth, and empower people through the free and open internet – in November 2018 IA established a London office to constructively engage in the internet public policy debate in the UK.

We are firm believers in the benefits that technology brings to everyday life and the economy, and for the potential that internet innovation has to transform society for the better. IA economic analysis shows that the internet sector contributes £45 billion to the UK economy each year, and is responsible for nearly 80,000 businesses and around 400,000 jobs. Recent IA polling found that 82 percent of British people believe that the internet had "made their lives easier and more enjoyable."

As the Government has made clear, the internet is now an integral part of everyday life and often a powerful force for good. Thanks to the internet, we now have unprecedented access to information, entertainment, communication and a vast range of new goods and services – which has created a more informed, connected and productive society. According to Ofcom data, the average person now spends 24 hours a week online, and multiple estimates have found that internet services create significant consumer surplus for ordinary people. Many of these services are provided to consumers free of charge, with the recent Bean Independent Review of UK Economic Statistics estimating that including the value created by free internet services in GDP would boost growth by 0.35 – 0.66 percentage points a year.

IA believes that the internet sector needs a balanced policy and regulatory environment to continue, and grow, its contribution to the UK economy, consumers and society in the future. The internet will drive 21st century prosperity, but there is a risk to this potential if policies and regulations are introduced which will damage the ability of the internet sector to: 1) drive UK economic growth; 2) provide services that people value highly; and 3) make a positive contribution to society.

IA and our members will continue to work constructively with policymakers and regulators on these important issues as the regulatory process continues.

2. Internet companies already take significant action to address harms

Internet companies support the broad approach to improving the regulatory environment to ensure the UK is the safest place in the world to be online. And while solving these problems is not easy - with tens of thousands of companies in scope ranging from social media, online forums, online marketplaces and more - as an industry we are committed to reducing harm online. Indeed, what is possible in relation to tackling harm is increasing every month. Internet companies take meaningful steps to protect their users from harm on their services, and over 45% of the public are now aware of the steps that companies take to keep people safe. 74% of the public also feel safe from harm when they are online, with just 4% saying they feel unsafe.

Company wide initiatives include:

- Investing significant resources in both human content moderation and, partnering with third sector organisations and think tanks, developing machine-learning technology to detect and remove harmful material more quickly.
- Working with groups like the Counter Terrorism Internet Referral Unit, and forming the Global Internet Forum to Counter Terrorism (GIFCT) to curtail the spread of terrorism and violent extremism online.
- Partnering with a number of organisations across the globe, including the Internet Watch Foundation, to work together to remove harmful CSAM from the internet.
- Forming internal online safety councils and designating employee teams to improve online safety and promote a productive and welcoming environment online.
- Creating clear pathways for people to report inappropriate or harmful content, so that it can be addressed under companies' terms and conditions.
- Investing in fact-checking services and using AI and other technology to tackle false information.
- Investing in educating users about how online services operate and how to make the best use of them. Efforts to educate people on what is appropriate on online platforms helps guide behaviour and can help minimise the need for moderation.

This is not to say that a simplistic focus on the amount of money invested in trust and safety initiatives or the number of content moderators employed by a company is the best or only means of assessing an organisation's commitment to safety. Indeed, different models of content moderation are used in industry to good effect – for example some services use a more community-based system of moderation or designed to address a certain type of content – and as the Bill recognises there should be different expectations on companies depending on their particular circumstances - including the reach or business models of organisations. Regulation should be proportionate in terms of the scale of harms prevalent on a service, and also in terms of the economic development stage and size of the platform.

Nevertheless, this is a hard problem, and no system of moderation, whether algorithmic or human, centrally-managed or community-based, will be perfect.

Some of the discussion around the release of the Government's Online Safety Bill continues to suggest that harm only persists on the internet because internet companies do not care or are not trying hard enough to tackle it. We fundamentally reject this characterisation – as set out above, internet companies have not waited for legislation and have taken, and will continue to take, significant steps to address harms on their services a. However, it is clear that there is not an easy or one-size-fits-all way for internet companies to instantly eliminate all online harms.

Alongside company efforts, there is also a role for government to provide industry and the public guidance on matters relating to public discourse, based on our laws and culture. Indeed, over 65% of the public are not aware of the proposed new regulation on online platforms - suggesting much work needs to be done to have a proper, public conversation to ensure we reach a positive outcome. The recently released Media Literacy Strategy was a welcome step in the right direction - but more must still be done. The expectations for behaviour online should be the same as for behaviour offline; and public institutions have a key role to play in establishing those norms, for example by following through on police investigations of criminal online harms, or providing online citizenship education through PSHE lessons in schools.

3. Key concerns with the Online Safety Bill

3.1 Duty of Care and senior management criminal liability

A Duty of Care model - which has been used in other areas of law - is much harder to apply for online spaces and will need to be approached with care in its application.

Following the suggestions of Woods and Perrin (2018,2019) and the NSPCC (2019), the Bill proposes a duty of care on internet companies to keep their users safe and tackle illegal and harmful activity on their services.

As is clear in its design, and made explicit in many of the third party reports calling for its introduction, much of the inspiration for the duty comes from Health & Safety Law. The 1974 Health and Safety at Work Act created a new duty of care for every employee to ensure "so far as is reasonably practicable, the health, safety and welfare at work of all his employees", which in turn was enforced by a new regulator, the Health & Safety Executive.

The 1974 Act is generally seen as a significant policy success - the UK is now one of the safest places to work in Europe - and it is understandable why policymakers have looked to it as a model for online harm.

Nevertheless, we also need to be clear about the ways in which online harms are not like the physical risks faced in the workplace:

- **Risks to physical health and safety are clearly defined, while online harms are much more ambiguous.** It is easy to ascertain when an employee has suffered a physical accident, and there are now well established methodologies for quantifying their seriousness in monetary terms. By contrast, many of the harms targeted by the Bill have a much less clear definition or boundary with other types of speech.

- **Without clear definitions, it is hard for companies to perform their own cost-benefit analysis and risk assessment.** A key element of the current health and safety regime is that while companies are encouraged to follow standard industry codes of practice, they are also allowed to, in effect, perform their own cost-benefit analysis of what risks are worth reducing. This is much less harder for online harms, leaving companies only able to follow agreed guidelines by the regulator - or to act as conservatively as possible. This is a particular risk for new or smaller companies, and could potentially act as a significant chilling effect on innovation.

- **There is no perfect technological solution that can completely eliminate the risk of all online harms.** In health and safety law our real worry is negligent employers - while many of the solutions and practices needed to ensure safety are relatively straight forward. When a practice is especially dangerous and risk is impossible to fully eliminate, governments tend to introduce more specific regulations specifically for that sector. For many online harms, by contrast, it is much less clear what the appropriate response in return is.

There are good reasons why we do not introduce legal duties of care whenever we have a policy goal. We do not introduce a duty of care for newspapers to ensure that their readers are perfectly informed, or a duty of care around environmental sustainability. While these are important societal goals, the way we have decided to tackle them is with specific regulations setting out very clearly the role of companies.

There are often hard trade-offs between different societal goals such as privacy, safety and innovation – and these need to be actively considered. Any duty of care model should focus on ensuring robust processes and systems are in place.

Indeed, the Lords Communications and Digital Committee's recent report laid out a view which would warrant further thought by the Government as it proceeds: "The duty of care approach should inform a flexible framework for digital regulation, guided by underlying principles, including freedom of expression, which is able to adapt to the rapidly developing digital world while setting clear expectations for platforms."

In relation to this issue is the inclusion of criminal liability for senior managers - though IA notes that this will not be introduced for at least two years after the regime is fully operational and only if services do not 'step up their efforts to improve safety'.

The UK has an ambition to become the safest place to be online - but also the best place to work and start a business in the thriving tech sector. But managerial liability and sanctions of the type held in threat through this Bill has the potential to make the UK less attractive to professional talent that is needed to help the UK's tech sector continue to grow - but also to innovate and find new ways to tackle online harms . It also has the potential to create a disincentive for anyone seeking to start or grow a new business here in the UK for fear of future criminal liability. It is our view that the threat of criminal liability must be completely removed from this process. As the Culture Secretary Oliver Dowden said himself in May 2021, "I would rather we didn't impose new criminal law".

3.2 Freedom of Expression

Freedom of expression online is underpinned in law by intermediary liability protections, which in a UK context are set out in the EU's e-Commerce Directive ("ECD"), as adopted into UK law. Articles 12-14 of the ECD contain protection from liability for those acting as "mere conduits", and those who are caching, or performing hosting services; and Article 15 prohibits general obligations being imposed on providers to monitor the information transmitted/stored, or actively to seek facts or circumstances indicating illegal activity.

The internet has also flourished in part because platforms permit users to post and share information without fear that those platforms will be held liable for third-party content. As it stands, the Bill has the potential to require internet companies to engage in over-censorship for fear of being held liable for content, with a consequential impact on freedom of speech - with blanket monitoring and proactive removal of content using automated tools the only route possible to meet the requirements. Intermediary liability protections also play a critical role in driving economic growth, by enabling new companies to invest and launch new services in the UK and enabling existing companies to innovate, scale and grow their businesses.

In its response to the 2012 Leveson Inquiry, the Government rejected the idea of statutory press regulation - arguing in effect that while there were real concerns about the harms created by the press, that introducing a statutory authority would compromise Britain's democratic traditions. In its last manifesto, the Conservatives confirmed their support of a "free and independent press", and pledged to repeal Section 40 of the Crime and Courts Act, which many have argued will have a disproportionate chilling effect on free speech.

While it is welcome that the Government has included the requirement for safeguards to be put in place to protect freedom of expression - it is likely that the reality will be very different based on the current proposals. And the duties on freedom of expression should be strengthened and given equal weight to the safety duties - with internet companies requiring more clarity about how these duties need to be balanced in practice.

Of particular concern is the independence for the regulator to decide the list of harms. While the initial list of illegal content has a focus on incitement to terrorism or violent extremism - which is already illegal and internet companies strongly agree with rooting out of our platforms - it is not hard to see the creation of a slippery slope as a precedent is created that the state can shut down any speech that it finds objectionable. Already we are seeing pressure to include in scope of the online harm duty of care books that argue for ideas we dislike.

Indeed, in its recent report, published on 22 July 2021, the House of Lords Communications and Digital Committee said that although it welcomes the Bill's proposals to oblige tech platforms to remove illegal content and protect children from harm, it does not support the government's plan to make companies moderate content that is legal, but may be objectionable to some.

Instead, the Lords argued that existing laws – such as those on harassment or grossly offensive publications – should be properly enforced, and any serious harms not already made illegal should be criminalised.

“We are not convinced that they are workable or could be implemented without unjustifiable and unprecedented interference in freedom of expression. If a type of content is seriously harmful, it should be defined and criminalised through primary legislation. It would be more effective – and more consistent with the value which has historically been attached to freedom of expression in the UK – to address content which is legal but some may find distressing through strong regulation of the design of platforms, digital citizenship education, and competition regulation.”

For example, by its very nature, political speech is often controversial - and encourages passionate disagreement. Part of freedom of speech is that we allow people to be wrong, and even to campaign for ideas that may have negative ideas for society. One person's fake news is another person's dissenting opinion. It is not the rule of publishers, platform owners or politicians to adjudicate these arguments - but the market of ideas and democratic debate. To give a relevant parallel, we do not think it would be appropriate to introduce a duty of care for publishers to avoid harm from reading their works.

Among liberal democracies, the UK is nearly alone in trying to introduce mandatory filtering of ideas disliked by a regulator or the state. However, by doing so, it is likely to set a worrying precedent that would encourage other authoritarian regimes such as Iran, China and Russia.

The Government has previously argued that the regulator should "not be responsible for policing truth and accuracy online". In practice, however, it will be hard for this safeguard to have teeth while maintaining the current and continued unspecified definition of legal but harmful content. While platform providers can perform a helpful moderation role, encouraging their audience to consume a variety of viewpoints, there is a significant difference between this and attempting to ban or censor speech.

3.3 Scope of services

While we speak of the Internet, in reality this covers a vast array of different services, run by companies and organisations of all sizes and models. The Government makes a deliberate choice to be as comprehensive as possible - and explicitly included in scope are companies and organisations "of all sizes" that "allow users to share or discover user-generated content or interact with each other online". Unlike many other types of regulation, there are no de minimus exceptions for small or new entrants.

In practice, however, there are significant differences between a public platform like YouTube and private messaging services. Many of the most popular messaging services, such as WhatsApp or iMessage, are end-to-end encrypted, making it technically impossible for platform owners to monitor the content of messages. Seeking to create a backdoor to read these messages would severely undermine individual privacy and severely undermine civil liberties. Just as the Royal Mail is not responsible for the contents of every letter, or telephone operators the contents of every call, we do not think it is proportionate to seek to regulate private communications in the same way as public communications.

While the Government explicitly recognises that private communications should be treated differently, it gives little guidance on what this will mean practically - or how 'private' is to be defined. Coming up with a workable definition is likely to be challenging. Many online

services already significantly blur the line between public: posts to your Facebook News Feed, for example, may be intended for an audience of friends and family in the hundreds, but still not for the Internet at large. And while Schedule 1 of the bill specifies certain services and content excluded from the scope of this regime - including emails, SMS messages and MMS messages - but the exclusion applies only if the services or content represents “the only user-generated content enabled by the service,” so Facebook Messenger, for example, does not qualify and it would be regulated.

The bill also gives significant power to the Government to amend Schedule 1 to add new services to the list of exemptions or remove some of those already exempt. This power gives Ministers a significant level of discretion, which, if misused in the future, could lead to policing private messaging and communications channels. While the main focus here would likely be illegal content such as terrorist and CSEA content, questions about the effect of the bill on encryption, security and privacy remain unanswered and will be important for the Government to clarify.

3.4 Legal but harmful content

The continued approach being taken by the Government surrounding ‘legal but harmful’ content has significant problems of subjectivity - especially around the definition that such content causes “physical or psychological harm”.

IA and other organisations have raised concerns about this - including how such harm can be proved in reality, and the evidence base that Ofcom will work from to assess this. The public share a similar concern - with 60% saying in a recent poll that the person who shared or created the content is ultimately responsible for it, with just 8% saying it is the responsibility of internet firms. This is not to say that internet companies are not responsible - but the public view here on how best to approach the improvement of behaviour online is important context.

Furthermore, 69% of the public agree that something is legal to say in person or to write down on a poster or in a newspaper, it should be legal to say online - which should act as a reminder to us all when drafting new regulation.

Given the enormous scope of activities undertaken on the Internet, the current proposals effectively give the proposed regulator enormous discretion to unanimously outlaw or discourage particular activities or types of speech. An important check and balance in a democracy is that when a society recognises a new problem, new law from Parliament or the courts is debated and argued rather than unilaterally implemented by the executive.

Indeed, many of the worst harms are already illegal, and despite rhetoric of a "wild west", internet companies are in reality already subject to a multitude of regulatory frameworks, designed to reduce the risk of loss of privacy, discrimination, monopoly, underage access to pornography, copyright infringement or misleading electoral campaigning.

Rather than a one-size-fits-all approach, we need to take each harm individually, and look for a proportionate response. Treating extremist content under the same framework as infinite scrolling pages ('designed addiction') risks criminalising legitimate speech and introducing massively disproportionate intervention.

For example, in recent years, there has been increasing concern about overuse of digital products - and the industry has worked to introduce new tools such as Android's Digital Well Being or iOS Screen Time to allow families to make their own choices about their digital health. Given that there is no clear evidence of a causal impact of excessive screen time on mental health - and as the Government acknowledges, significant evidence of a positive impact from being online for a majority of children and young people - we believe that this is not a proportionate response. While we should continue to monitor and commission new evidence, we do not believe that there are good reasons to treat the pure use of online services in the same category as terrorist content, extreme pornography or hate crime.

In order to avoid mission creep, we believe that at minimum the new regulator should be required to provide an updated list of the specific harms it is concerned with and the evidence base lying behind them. A better safeguard still, however, would be for the regulator to be given a specific list of harms to address, which could then be revisited on a recurring basis. Beyond helping focus the work of the regulator, this would give significantly greater clarity for internet services - and help to protect against the regulatory framework being used for state censorship.

3.5 Economic growth and international impact

The Government has been keen to emphasise that innovation and safety online are not mutually exclusive. But as history has told us, the hardest hit by new regulations are often smaller companies and start-ups, who find it harder to absorb the fixed costs of new administrative systems. While the Government argues that we can learn from the example of other areas of regulation such as GDPR or Health and Safety rules to reduce the burden on SMEs, it is misleading to argue that these did not create significant costs for businesses. (The Federation of Small Businesses website, for example, reports that "Ensuring your business is compliant with all the relevant health and safety regulations is a time consuming and costly process".) By creating additional costs, new regulations increase barriers to entry, making it harder for disruptive new entrants.

The Bill states that the regulator will take a proportionate approach, taking account of the size of companies and the reach of their platforms. This is a good idea - but given that there is no fixed list of harms, and the details of every company is likely to be subtly different, it is going to be difficult to completely remove ambiguity over what is required to be compliant, particularly for companies developing new and innovative products. Given the new proposed liability for significant fines, many companies are going to err on the side of an extremely risk averse approach.

One particular worry is that in practice, the only way to meet many of the demands of a new duty of care will be through the introduction of mandatory filtering. Beyond the potential impact on free expression, this kind of content filtering can be extremely expensive to develop and iterate - and often needs to be complemented by significant amounts of human moderation.

Structurally, a duty of care risks embedding a 'precautionary principle' within regulation of the Internet. While the precautionary principle can be appropriate in areas of high risk or it is hard to reverse damage, as in environmental sustainability, neither of these cases applies to many of the kinds of harms targeted by the Bill. The precautionary principle is not an

appropriate benchmark for all regulation, and taken literally, as leading legal scholars have argued, is likely meaningless - both inaction and action create risks. As many commentators have argued, one of the reasons the internet has delivered significant beneficial new services in the last few decades is an approach of 'permissionless innovation', allowing small teams to try out new ideas rather than have to seek permission from large bureaucracies or a government regulator first.

As well as slowing future innovation, these rules could lead to a worsening of the quality of Internet services consumers already receive. As we have already seen to some extent with GDPR, many foreign platforms and publishers will often decide it is easier to block access in the UK rather than incur extra costs or liability. Even for the larger platforms, the loss of effective intermediary liability protection could make it cost prohibitive to keep offering the same kinds of service.

The best way to avoid this chilling effect on innovation is to ensure that any remedies are based around a specific list of harms, with a clear evidence base of harm and a quantified regulatory impact assessment of best practice in reducing risk. This will require the Government to make some hard decisions about trade-offs between different values upfront – but it is better to do this now, than leave potential ongoing ambiguity and the possibility of a slippery slope to continued restrictions.

It will also make it easier for companies to focus resources on innovating on the most important harms. It is in everybody's interests to create a safer internet – and the best way to do that is if we work together to keep innovating on new, scalable and cost effective ways of identifying hostile actors, providing users with a balanced range of content, and protecting individual privacy.

As a global organisation with representation in both the US and the UK, IA is well placed to make a judgement on the impact the Bill will have on the UK globally. The world looks up to the UK; indeed, the Government has an ambition for any new regulation of the internet to be a “world-leading” example for other nations to follow. However, we must be clear that the way we proceed on rules around legal but harmful content, or potential fines or criminal liability for tech staff may well be followed by governments around the globe - good or bad.

As the Bill continues to be assessed, we must continue to ensure it could not be used as a reason for authoritarian nations, autocratic leaders, and nations with state-restricted internet to impose their own chilling effects on citizens.

Instead, we should focus on our strengths. The US and UK both have vibrant digital economies and strong commitments to the open internet. One sign of the strong, reciprocal digital trade relationship between our two countries is that both are the most important cross-border e-commerce markets for each other, and both are world leaders in digital exports. The U.S. now exports $48.8 billion (£39 billion) in digital services to the UK, an increase of 52 percent from 2006 to 2018. Similarly, the UK now exports $34.8 billion (£27.8 billion) to the US, an increase of 56 percent from 2006 to 2017. The US and the UK also rank numbers five and six, respectively, among OECD countries for their share of predominantly digitally-delivered services in commercial services trade. And nearly one fifth of each economy’s total employment is in ICT task intensive jobs.

Importantly, those digital exports are not just the products of large technology companies. Roughly a quarter of manufacturing exports are enabled by digitally-intensive services. Online e-commerce platforms also enable a small business on main street or the high street to export to customers around the world. And online ratings and reviews offer a key signal to online shoppers as they look to make a purchase, with more than two-thirds of US consumers saying they check online ratings and reviews either “every time” or “most of the time” before visiting a business or making a purchase online, while in the UK online reviews are as important to consumers as recommendations from friends and family when making purchases.

It sets a crucial example for other countries to follow. At a time when countries like China, India, and Russia are pushing very different, closed visions of the internet, it is crucial for our two countries to coalesce around best-in-class international digital regulation for the 21st century. Getting this Bill right forms a key part of this.

27 September 2021