Internet Association – Response To Online Harms White Paper Consultation

1. Introduction

Internet Association ("IA") welcomes the opportunity to respond to the joint DCMS and Home Office consultation on the Online Harms White Paper ("OHWP").

IA represents over 40 of the world's leading internet companies[1] 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.[2] Recent IA polling found that 82 percent of British people believe that the internet had "made their lives easier and more enjoyable."[3]

As the OHWP argues, 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,[4] and multiple estimates have found that internet services create significant consumer surplus for ordinary people.[5] 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.[6]

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 has previously proposed a number of regulatory policy principles which we believe can help deliver this balanced environment, and IA and our members will continue to work constructively with

---

[1] IA Member Company List: https://uk.internetassociation.org/our-members/
[2] https://uk.internetassociation.org/publications/measuring-the-uk-internet-sector/
[3] https://uk.internetassociation.org/internet-association-launches-uk-presence-with-poll-showing-overwhelming-public-backing/
[4] https://www.ofcom.org.uk/__data/assets/pdf_file/0022/117256/CMR-2018-narrative-report.pdf
[5] https://www.pnas.org/content/116/15/7250
[6] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/507081/2904936_Bean_Review_Web_Accessible.pdf

policymakers and regulators on these important issues as the White Paper process continues.

1.1 Internet Companies Take Significant Action To Address Harms

As an industry we are absolutely committed to reducing harms. Nobody wants the internet to be a place where anyone feels unsafe, or users are misled. We recognise that there are legitimate concerns about illegal and harmful content, and internet companies take meaningful steps to protect their users from harm on their services. Initiatives include:

- Investing significant resources in both human content moderation and, partnering with third sector organisations and researchers, developing machine-learning technology to detect and remove harmful material more quickly.
- Working closely with law enforcement, 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.
- 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.

The internet sector is not a homogenous entity – a critical point to note – so tailoring approaches to the type of service and/or harm is key to an effective response. As a result, the industry takes a diversity of approaches to tackling online harms – the wide range of services and business models means there is no one-size-fits-all approach, and we cannot simply focus on the amount of money invested in trust and safety initiatives or the number of content moderators employed by a company as 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 – and as the OHWP recognises there should be different expectations on companies depending on their particular circumstances. Regulation should be proportionate in terms of 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 OHWP has appeared 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 take significant steps to address harms on their services and know there is more to be done. However, we believe the public debate should acknowledge that there is no easy way for internet companies to instantly eliminate all online harms.

Alongside company efforts, there is also a role for government to provide guidance to industry and the

public on matters relating to public discourse, based on our laws and culture. Moral and ethical judgements on content are closely entwined with fundamental rights to free expression, a private life and freedom to access information. As such, they should not be delegated to private companies, and require clarity from government on the appropriate frameworks for regulating speech online. Under the UN Guiding Principles on Business and Human Rights, governments have a duty to protect the human rights of their citizens, including from violation by companies. The UK government's ambition to be a world leader in the regulation of online harms, at a time when malign actors are increasingly using the internet to attack democratic institutions and values, means that the UK government will have to show leadership in its commitment to protecting human rights online.

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.

We need to keep working together to make the internet safer. In order to further reduce online harms, we will need private and public sectors to work together – and to make use of a variety of tools, including technology, public education, the law and better regulation.

1.2 Internet Association Online Harms Regulatory Principles

As part of our engagement with government, IA and its member companies agree with the importance of proportionate regulation and previously proposed a number of regulatory policy principles to help achieve this outcome.[7] In order to meet our shared ambitions on internet safety, and the government's Digital Charter goal to make the UK the most attractive place to start up and grow an internet company, we believe that this regulation should:

- Be targeted at specific harms, using a risk based approach;
- Provide flexibility to adapt to changing technologies, different services and evolving societal expectations;
- Maintain the intermediary liability protections that enable the internet to deliver significant benefits for consumers, society and the economy;
- Be technically possible to implement in practice, and also take into account that resources available for this type of activity vary between companies (i.e. solutions are commercially possible);
- Provide clarity and certainty for consumers, citizens and internet companies;
- Recognise the distinction between public and private communications.

IA hopes that these principles have been useful so far, and we encourage the government to take more account of the principles – in particular the importance of maintaining intermediary liability protections – as the OHWP process continues.

[7] https://uk.internetassociation.org/blog/online-harms-regulatory-principles/

2. Internet Association Comments On The OHWP

2.1 Points To Welcome

IA welcomes a number of positive elements in the OHWP that should be incorporated into any future policy and regulation in this area.

2.1.1 Commitment To A Free And Open Internet, And A Thriving Digital Economy

The government states in its overall vision that it wants to ensure "a free, open and secure internet", that it wants to protect "freedom of expression online" and that it would like to see "the UK as a thriving digital economy, with a prosperous ecosystem of companies developing innovation in online safety".[8] IA supports these ambitions, and encourages the government to increase its focus on ensuring that any regulation delivers these important objectives relating to freedom, democracy and the economy.

2.1.2 Commitment To Regulatory Clarity

IA welcomes the government's ambition to provide "clarity to companies".[9] This is aligned with IA's own principle that any regulation should provide "clarity and certainty for consumers, citizens and internet companies", and is also aligned with the growing view that the government should be more clear on the appropriate frameworks for regulating speech online. IA hopes that the OHWP process will lead to more clarity in key areas – in particular on "harms with a less clear definition" – to reduce uncertainty for consumers and companies.

2.1.3 Commitment To A Risk-Based And Proportionate Approach

The government states that: it is committed to a "risk-based and proportionate approach";[10] a "key element of the regulator's approach will be the principle of proportionality";[11] and "the government will require the regulator to adopt a risk-based approach".[12] IA agrees that any regulation needs to be risk-based and proportionate – in terms of scale of harms prevalent on a service, and also in terms of the economic development stage and size of the platform.

2.1.4 Due Regard To Innovation

The government proposes a legal duty on any regulator to "pay due regard to innovation, and to protect users' rights online, taking particular care not to infringe privacy or freedom of expression".[13] IA agrees that it is vital that any regulation – or regulator – does not stifle innovation or undermine people's rights.

[8] Paragraph 12
[9] Paragraph 13
[10] Paragraph 31
[11] Paragraph 3.4
[12] Paragraph 5.3
[13] Paragraph 36

2.1.5 Recognition Of Existing Online Regulation

IA welcomes the government's recognition that there is already an existing base of regulation aimed at online harms and services.[14] The government cites the ICO and GDPR, the EHRC and equality and freedom of expression, Ofcom and video-on-demand services, the CMA and consumer protection law, and the forthcoming EU Audiovisual Media Services Directive, as examples among a range of legislation and regulation currently covering the internet. While the government views this as a "fragmented" landscape, we welcome the recognition in the first instance that the internet is not currently an unregulated "wild west", and that implicitly there is a base of regulation on which to build.

2.1.6 Role Of Technology And Digital Literacy

IA supports the OHWP's general ambitions for technology to play a key role in helping people stay safe online, as set out in Section 8, and for the role of digital literacy in improving online interactions, as set out in Section 9. In particular, the proposal for a new online media literacy strategy is welcome and will ideally not only help people develop the skills to safely navigate the online word, but will also increase digital civility and make it clear to people that the required standards of behaviour offline also apply online. IA agrees that all parties should focus on improving media literacy, and these efforts should receive similar levels of attention that issues around content moderation currently receive.

2.2 Overarching Concerns

While there are many points to welcome in the OHWP, IA has the following overarching concerns with the proposals.

2.2.1 Not sufficiently targeted or proportionate

IA remains concerned that, in contrast to the stated ambition to be risk-based and proportionate, the current proposals in the OHWP – particularly around the duty of care, scope, and draft codes of practice – are not sufficiently targeted or proportionate to the harms they are designed to minimise. As other commentators have argued, there is a real risk these proposals hurt the British tech sector, worsen the quality of internet services for ordinary consumers, undermine privacy, and produce a chilling effect on freedom of speech.

2.2.2 Does not seek to address harms holistically

We believe that we should collectively focus on addressing harms holistically – tackling societal problems both at their root in the real world, as well as in their online manifestation. Internet companies want to play their part in solving these issues, but technology is not the root cause of the harms addressed in the paper. As such, we believe that a broader policy approach, looking both offline and online, will lead to better outcomes for society.

[14] Paragraph 2.5

2.2.3 Potentially imposes a de facto general monitoring requirement

The OHWP states that the proposals are "compatible with the EU's e-Commerce Directive"[15] and that there will not be a "general monitoring" requirement on companies.[16] However, we are highly concerned that, in aggregate, the proposed regulator framework may undermine the intermediary liability protections that have enabled the internet to deliver significant benefits to the UK. We are very keen to explore further the interaction of the OHWP and relevant EU Directives to better understand the implications.

The internet has 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. Dilution of intermediary liability protections would encourage internet companies to engage in over-censorship for fear of being held liable for content, with a consequential impact on freedom of speech. 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.

2.3 Internet Association's Initial Response

In IA's initial response to the OHWP of 29 May 2019, we set out five specific concerns with the proposals. We appreciate that these points have been noted by officials, but we provide a slightly updated summary of them here again for completeness:

- "Duty of Care" has a specific legal meaning that does not align with the obligations proposed in the OHWP, creating legal uncertainty, and would be unmanageable;
- The scope of the services covered by regulation needs to be defined differently, and more closely related to the harms to be addressed;
- The category of "harms with a less clear definition" raises significant questions and concerns about clarity and democratic process;
- The proposed code of practice obligations raise potentially dangerous unintended consequences for freedom of expression;
- The proposed measures will damage the UK digital sector, especially start-ups, micro-businesses and small- and medium-sized enterprises (SMEs), and slow innovation.

2.3.1 "Duty of Care" has a specific legal meaning that does not align with the obligations proposed in the OHWP, creating legal uncertainty, and would be unmanageable.

The new statutory duty of care on internet companies is proposed "to take reasonable steps to keep their users safe and tackle illegal and harmful activity on their services." As is clear in its design, much of the inspiration for the duty comes from Health & Safety and Occupiers' Liability Law. It is understandable why policymakers have looked to these examples as models for online harm, but there are limitations in these comparisons and in particular 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

[15] Paragraphs 41 and 6.14
[16] Paragraph 3.12

ambiguous. It is easy to ascertain when an employee has suffered a physical accident, but many of the harms targeted by the OHWP, such as cyberbullying and trolling, extremist content or disinformation, 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 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 analysis of what risks are worth reducing. This is much harder for online harms, leaving companies only able to follow agreed guidelines by the regulator – or to act as conservatively as possible.
- There is no perfect technological solution that can completely eliminate the risk of all online harms. In health and safety law the 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 required.
- For online harms, we need to consider not only the role of companies, but also the role and responsibilities of individuals using the online service. In health and safety we are concerned mainly with the relation between the employer and employee, or the role of the provider of a public facility, but for online harms we need to look at the responsibilities of both the online services and the users that upload the harmful content itself – and the direct interactions between users themselves.

2.3.2 The scope of the services covered by regulation needs to be defined differently, and more closely related to the harms to be addressed.

Online services vary widely in business model; any new regulation must address this. There are significant differences between a social media platform, a search engine, a review website, an online marketplace, a fan forum, a cloud service, or a private messaging service. Moreover, there needs to be closer consideration of where harms are actually occurring online and then regulatory focus should be targeted at where the harm exists, rather than across a wider range of services.

There should be a clear distinction between private and public communication in the regulation, and monitoring of private communication should not be considered without robust public and parliamentary debate. Seeking to create a backdoor to read private messages would also severely undermine individual privacy and severely undermine civil liberties. While the OHWP 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. There should not be a fundamental change to how private communications can be monitored without a serious public debate on the implications.

2.3.3 The category of "harms with a less clear definition" raises significant questions and concerns about clarity and democratic process.

Rather than provide a specific list of harms it seeks to tackle, the OHWP instead only definitively sets out what harms are not in scope: harms to organisations, breaches of privacy or security, and harms suffered from using the dark web rather than open internet. Given the wide scope of activities undertaken on the internet, this effectively gives the proposed regulator enormous discretion to unanimously outlaw or discourage particular activities or types of speech. We believe it is important that

key decisions about internet regulation and freedom of speech are made by Parliament after thorough and reasoned debate.

2.3.4 The proposed code of practice obligations raise potentially dangerous unintended consequences for freedom of expression.

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. However, by explicitly including disinformation within scope and referring to the harms created by inaccurate information – "regardless of intent" – the new measures risk introducing state regulation of the press by the backdoor.

The OHWP rightly argues 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 unspecified definition of online harms. 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.

2.3.5 The proposed measures will damage the UK digital sector, especially start-ups, micro-businesses and small- and medium-sized enterprises (SMEs), and slow innovation.

The OHWP is keen to emphasise that "innovation and safety online are not mutually exclusive" and proposes to give the new regulator a legal duty "to pay due regard to innovation", pointing to a similar obligation placed on the ICO under the Data Protection 2018.[17]

The hardest hit by new regulations are smaller companies and start-ups, who find it harder to absorb the fixed costs of new administrative systems. While the OHWP 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 OHWP argues that the regulator will take a proportionate approach, taking account of the size of companies and the reach of their platforms. But given that there is no fixed list of harms, and the details of every company are likely to be subtly different, it is going to be difficult to completely remove ambiguity over what is required to be compliant. Given the new proposed liability for significant fines, many companies are going to err on the side of an extremely risk averse approach.

[17] It is too early to assess how this duty has been fulfilled by the ICO, and in any case the ICO is implementing GDPR obligations, which are implemented across all member states, thereby reducing the negative international competitiveness element of the regulation, while the OHWP obligations would only be implemented in the UK.

2.4 Further Specific Concerns

IA has undertaken further analysis of the OHWP, and identified a number of additional points for consideration.

2.4.1 Enforcement Regime

IA is concerned that the enforcement regime set out Section 6 is disproportionate and will have a chilling effect on internet innovation and freedom of expression in the UK. As with any regulation, there of course needs to be the threat of sanctions to act as a deterrent, but we are concerned that the OHWP proposals go well beyond what is necessary to ensure compliance.

As the government notes, the proposed powers in Paragraph 6.4 of the OHWP (i.e. civil fines, requiring remedial action, requiring information, naming and shaming) are fairly standard across regulated industries. However, we believe the thresholds for taking these actions (in particular issuing fines or naming and shaming), as well as the financial value of the penalties (with respect to civil fines) need to be more clearly defined. For example, we would only expect fines to be issued in the most serious cases of non-compliance, and we would expect there to be reasonable limits on the level of fines that could be imposed.

The government also consults on further, more novel enforcement powers, such as "disruption of business activities", ISP blocking, and senior management liability. IA is concerned that these powers are disproportionate and inappropriate. In particular, senior management liability, combined with the extensive "duty of care" obligations, would have the practical impact of discouraging UK companies from launching internet businesses, and discouraging global internet companies from establishing operations in the UK. It would also provide a disincentive for existing businesses to continue to provide their services in the UK, which would be detrimental to people who use and enjoy a wide range of internet services.

2.4.2 Potential Creation Of A Private Right Of Action

In addition to our general points on the "duty of care" concept, set out in Section 2.3.1 above, we are concerned that the proposal risks creating a private right of action for consumers against companies. The creation of a private right of action would be a disproportionate response to the issue of online harms, and IA believes that any further internet regulation in this area should not establish such a right.

Rather than a private right of action, IA believes that redress is more appropriate through an expert regulator with technology expertise, who can bring consistency to enforcement, and transparency around enforcement for public accountability and for raising the level of compliance among covered companies.

2.4.3 Transparency Reporting Powers

IA member companies have made clear their resolve to provide more and more meaningful transparency to their users and to the wider public. Many IA member companies publish extensive transparency data on their internet safety practices, terms and conditions, and systems for content flagging and removal.

However, IA has a number of concerns with the proposed transparency reporting powers in the OHWP. While it will be for the regulator to decide what information it requires, we flag at this stage considerations about the level of detail potentially required, timing challenges with the provision of information; and the ability of smaller companies to comply with detailed requirements. We are also concerned about the proposed power of the regulator to "require additional information" from companies to "inform its oversight of enforcement activity", which is not clearly defined and could be used to justify disproportionate information requests.

In addition, IA would be very concerned if this power was used to require companies to publicly disclose explanations about the way algorithms operate. IA members companies are already engaging in transparency around rankings and why content appears – for example by providing overviews of how their platforms operate. However, algorithms are often the IP of internet companies, and are what make them unique and different from competitors. In a free and open economy, sharing confidential business information such as this would be unfair. Further, algorithms help platforms tackle bad actors. IA it believes it is important to ensure that these bad actors are not empowered with information that enables them to act inappropriately. For all these reasons, we are concerned about calls for algorithmic transparency that would diminish the user experience and empower bad actors.

More broadly on the point of commercial sensitivity and information disclosure, we encourage policymakers to carefully consider the level information that may be required for the regulator to perform its functions, and which can be provided in private, versus information that may be required for distribution to the wider public.

2.4.4 Code Of Practice Requirements

Section 7 of the OHWP sets out how companies would need to fulfil the duty of care across different harms, including "expectations" which would then be developed by the regulator into codes of practice. IA welcomes the recognition by government that different harms require different solutions, and that not all expectations may be applicable to every company. However, we have a number of concerns with the code of practice framework proposed in the OHWP.

First, while the OHWP explicitly recognises the need for different solutions, it is a consistent theme across the codes of practice that companies in scope are required to proactively identify, prevent and/or remove content in the various categories of harm. We are concerned that this one-size-fits-all solution is not sufficiently targeted and does nor recognises the differences in approach needed across different harms.

Second, we are concerned that the "expectations" on companies across the categories of harm are very prescriptive, rather than principles-based, and would result in regulation that was contrary to the government's stated objectives of proportionality and delivering a risk-based approach. IA believes that it is more appropriate to focus on the requirements on companies in terms of the standards and process they adopt, rather than prescriptive obligations for action.

Third, while technology is rightly part of the solution, there are limitations to what can be achieved through technical means. For example, in areas where context is important, human review will be required in order to help ensure reasonable outcomes. For services such as live-streaming, there is not a technical means of moderating this content before it appears on a platform. While internet companies

will continue to innovate with technical solutions, we believe that there needs to be further consideration of the technical feasibility of proposed "expectations" in the codes of practice.

Fourth, we are concerned that the OHWP proposes that the regulator establish multiple codes of practice (the OHWP references 11 code areas), which could lead to uncertainty and a lack of clarity for companies. There is a risk that the codes could conflict with each other, or conflict with existing laws, and a complicated multi-code framework would make it difficult for companies to comply with the duty of care requirements.

2.4.5 Regulator Costs

IA notes the government intends for the regulator to be cost neutral to the public sector. While it is fairly normal practice for the cost of establishing and running a regulator to be recovered from industry, IA would be concerned if any industry levy went beyond the purpose of cost-recovery for the regulator, or if any regulator was reliant on income from financial penalties to fund its activities.

In addition, we believe it is important to consider the wider impacts of any new industry levy. In particular, the risk that new costs may have the effect of displacing existing industry spend on industry safety initiatives, and the risk that new costs may push smaller companies out of the market or hinder larger companies from continuing to grow.

IA also encourages the government to think holistically about new direct and indirect costs imposed on industry to ensure that various discrete costs (for example, regulator levy, Digital Services Tax, voluntary industry contributions to tackle harms), which are being considered in isolation, do not amount to an unreasonable burden when looked at cumulatively.

3. Recommendations To Consider

Since launching in the UK in November 2018, IA has engaged constructively with the government on internet policy issues, and wants to continue to make positive contributions to the policy discussion. In this context, we would like to suggest a number of recommendations for the government as it considers next steps on the OHWP.

3.1 Process

IA encourages the government to reflect on the concerns raised by industry in relation to the OHWP, and further consider IA's regulatory policy principles. This is a complex area – various trade-offs will be required – and sufficient time needs to be set aside for policymakers, industry, the general public and civil society stakeholders to consider the issues in the round to achieve a balanced outcome.

We believe the government should commit to taking the time necessary to consider these complex policy and social issues fully. Should the government proceed with its stated intention of introducing legislation, IA believes that the government should commit to undertaking formal pre-legislative scrutiny of the bill.

3.2 e-Commerce Directive

IA encourages the government to seriously consider industry's concerns around intermediary liability protections and the OHWP, and in particular: a/ the potential imposition of a de facto general monitoring requirement; or b/ any dilution of intermediary liability protections.

We ask the government to publish its legal advice on the compatibility of the OHWP with the e-Commerce Directive so that industry can assess the inter-relationships and risks involved. In relation to any future regulation in this area, IA believes that the government should offer solid guarantees to industry that UK regulation will not undermine the intermediary liability protections that have underpinned the internet economy.

3.3 Impact Assessment

IA and its member companies share the government's ambition to make the UK the safest place in the world to be online. We also share the government's ambition for the UK to be the best place in the world to run a digital business. We believe the government should give further consideration to the economic element of its ambitions, to avoid regulation that has a significant negative impact on the UK economy in general, digital businesses in particular, and consequently on internet services that consumers rely on. We also encourage the government to take greater consideration of impacts on freedom of expression and privacy.

We recommend that the government undertakes a full regulatory impact assessment of the White Paper proposals, covering the economic impact (in particular the impact on start-ups and small- and medium-sized enterprises) and impacts on freedom of expression and privacy.

3.4 Regulatory Framework

IA has raised a number of specific concerns about the proposed regulatory framework, in particular the legal definition of "duty of care", the services in scope, and the harms in scope.

We believe that the best way to avoid unbalanced and disproportionate regulation 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 on speech or negative economic effects.

We believe that government should consider tried and tested models of oversight, that includes the input of subject-matter experts from industry. In keeping with its desire to encourage innovation, and maintain meaningful protections for free expression and ensure that regulation is up-to-date and effective, the government should also consider solutions where the desired outcomes are managed through self-regulation or co-regulation, with the participation of experts in the industry. This should be informed by European and international digital accountability and co-operation models, as well as the UK's experience in other industries such as advertising.

Specifically on the scope of the services covered by the OHWP, one solution on scope could be to exclude specific types of services where the risk of harm is low, or where it is not feasible for companies to be subject to the regulatory framework. A good example of this latter case is cloud services provided to enterprise customers. Cloud companies have neither the technical, legal nor moral capacity to monitor and report on their customers' content – they could, in effect, be asked to wiretap their customers. This is a crucial aspect that needs to be addressed at the outset otherwise it will create substantial concern among all companies in the UK seeking to invest in modern IT services.

4. Concluding Comments

IA welcomes the opportunity to respond to the OHWP. IA and its member companies are committed to reducing online harms and believe that there is a role for targeted, proportionate online safety regulation. However, IA has a number of significant concerns with the OHWP proposals.

IA supports balanced, proportionate regulation that achieves the joint objectives of protecting people from harm online and ensuring that the internet can continue to deliver benefits to the economy and society. IA has proposed a number of regulatory policy principles which it believes can help deliver this outcome, and IA and its members will continue to work with policymakers and regulators on these important issues as the White Paper process continues.

Annex: Consultation Questions

Question 1: This government has committed to annual transparency reporting. Beyond the measures set out in this White Paper, should the government do more to build a culture of transparency, trust and accountability across industry and, if so, what?

IA member companies have made clear their resolve to provide more and more meaningful transparency to their users and to the wider public. Many IA member companies publish extensive transparency data on their internet safety practices, terms and conditions, and systems for content flagging and removal.

However, IA has a number of concerns with the proposed transparency reporting powers in the OHWP. While it will be for the regulator to decide what information it requires, we flag at this stage considerations about the level of detail potentially required, timing challenges with the provision of information; and the ability of smaller companies to comply with detailed requirements. We are also concerned about the proposed power of the regulator to "require additional information" from companies to "inform its oversight of enforcement activity", which is not clearly defined and could be used to justify disproportionate information requests.

In addition, IA would be very concerned if this power was used to require companies to publicly disclose explanations about the way algorithms operate. IA members companies are already engaging in transparency around rankings and why content appears – for example by providing overviews of how their platforms operate. However, algorithms are often the IP of social media platforms, and are what make them unique and different from competitors. In a free and open economy, sharing confidential business information such as this would be unfair. Further, algorithms helps platforms tackle bad actors. IA it believes it is important to ensure that these bad actors are not empowered with information that enables them to act inappropriately. For all these reasons, we are concerned about calls for algorithmic transparency that would diminish the user experience and empower bad actors.

More broadly on the point of commercial sensitivity and information disclosure, we encourage policymakers to carefully consider the level information that may be required for the regulator to perform its functions, and which can be provided in private, versus information that may be required for distribution to the wider public.

Question 2: Should designated bodies be able to bring 'super complaints' to the regulator in specific and clearly evidenced circumstances?

IA believes that it is an effective and sufficient form of redress for individuals to bring complaints to companies directly in line with their terms and conditions/internal complaint processes.

In addition to our general points on the "duty of care" concept, set out in Section 2.3.1 above, we are concerned that the proposal risks creating a private right of action for consumers against companies. The creation of a private right of action would be a disproportionate response to the issue of online harms, and IA believes that any further internet regulation in this area should not establish such a right.

Rather than a private right of action, IA believes that redress is more appropriate through an expert regulator with technology expertise, who can bring consistency to enforcement, and transparency

around enforcement for public accountability and for raising the level of compliance among covered companies.

Question 2a: If your answer to question 2 is 'yes', in what circumstances should this happen?

N/A

Question 3: What, if any, other measures should the government consider for users who wish to raise concerns about specific pieces of harmful content or activity, and/or breaches of the duty of care?

IA believes that it is an effective and sufficient form of redress for individuals to bring complaints to companies directly in line with their terms and conditions/internal complaint processes.

Question 4: What role should Parliament play in scrutinising the work of the regulator, including the development of codes of practice?

IA believes that the proposed codes of practice obligations raise potentially dangerous unintended consequences for freedom of expression.

Wherever governments want to restrict speech, they should use democratic processes to clearly outline the case. The current proposal risks allowing a regulator to limit access to legitimate information in an opaque and arbitrary manner, in effect banning speech without openly declaring it unlawful or providing clear definitions of what is and is not permissible.

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 misinformation is another person's dissenting opinion. It is not the role 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 book publishers to avoid harm from reading their works.

IA therefore believes that Parliament should play an active role in debating and setting policy when it comes to issues such as freedom of expression, which should not be simply delegated to an unelected regulator. Parliament should also have the opportunity to debate any proposed dilution of the right to privacy of communications, for example obligations which amount to wide monitoring of private communications The internet industry is committed to addressing illegal harms, but we are also concerned about government imposing specific codes of practice in advance of debate of these matters in Parliament.

Finally in this area, IA believes that regulator should be required to undertake meaningful consultation with industry on proposals, such as draft codes of practice.

Question 5: Are proposals for the online platforms and services in scope of the regulatory framework a suitable basis for an effective and proportionate approach?

IA believes further work needs to be done to ensure a suitably effective and proportionate response to online harms. See Sections 2.2, 2.3 and 2.4 of this response.

Question 6: In developing a definition for private communications, what criteria should be considered?

As set out in our regulatory principles of 28 February 2019, IA believes that any future online safety regulation should recognise the distinction between public and private communications, and the implications of government involvement in the latter. The reach and impact of communications online differs according to the service used. A service that enables one-to-one private communication between individuals is different to a service that plays out communication to the public, which is different again to a service that provides information in response to a consumer request. While regulation quite rightly has a role to play in relation to public communications, care should be taken to avoid regulation encroaching into the surveillance of private communications, which should be a matter for individuals.

Seeking to create a backdoor to read private 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. In addition, many of the most popular messaging services are end-to-end encrypted, making it technically impossible for platform owners to monitor the content of messages.

Further, private communications are protected from government intervention in numerous laws, and interception is permitted under Investigatory Powers Act. The OHWP explicitly recognises that private communications should be treated differently. IA believes that private communications should be out of scope of the OHWP.

Question 7: Which channels or forums that can be considered private should be in scope of the regulatory framework?

IA believes that private communications should be out of scope of the OHWP.

Question 7a: What specific requirements might be appropriate to apply to private channels and forums in order to tackle online harms?

IA believes that private communications should be out of scope of the OHWP.

Question 8: What further steps could be taken to ensure the regulator will act in a targeted and proportionate manner?

Should the government establish a regulator, it will be important to introduce specific duties in law to ensure it will act in a targeted and proportionate manner. For example, the government could codify its statements in the OWHP that: it is committed to a “risk-based and proportionate approach”; a “key element of the regulator’s approach will be the principle of proportionality”; and “the government will require the regulator to adopt a risk-based approach”. IA agrees that any regulation needs to be risk-based and proportionate – in terms of scale of harms prevalent on a service, and also in terms of the economic development stage and size of the platform.

The government proposes a legal duty on any regulator to “pay due regard to innovation, and to protect

users' rights online, taking particular care not to infringe privacy or freedom of expression". IA believes that it is vital that any regulation – or regulator – does not stifle innovation or undermine people's rights. The current OHWP proposals provide a significant disincentive to innovation and present risks to both privacy and freedom of expression, in particular due to the proposed scope and draft codes of practice obligations.

In practical terms, further steps that could help ensure targeted and proportionate actions include:

- Including industry representatives on the regulator's Board; and
- Requiring the regulator to undertake meaningful consultation with industry on proposals, such as draft codes of practice.
- Requiring the regulator to act proportionately when using its information gathering powers. For example, we are concerned about the proposed power of the regulator to "require additional information" from companies to "inform its oversight of enforcement activity", which is not clearly defined and could be used to justify disproportionate information requests.

Question 9: What, if any, advice or support could the regulator provide to businesses, particularly start-ups and SMEs, comply with the regulatory framework?

IA believes that it may be helpful for the regulator to encourage the wider use of technology developed by larger actors to enable smaller actors to use these resources to tackle online harms (e.g. shared databases/open source approaches). However, the regulator should be cautious about mandating usage of these tools. IA also believes it would be helpful for the regulator to also support the creation of more partnerships with well-established third-party organisations and civil society groups that have the expertise in dealing with certain types of online harms.

Question 10: Should an online harms regulator be: (i) a new public body, or (ii) an existing public body?

At this point, IA believes that it is more important to consider the regulations themselves rather than "who" a regulator might be. IA encourages the government to reconsider the overall OHWP proposals in the light of feedback from industry and other groups, and once further progress is made on targeted, proportionate regulation then the sequencing is right to consider the identity of any regulator.

That said, IA believes that any regulator would need: the right staff and expertise to operate effectively; appropriate duties that allow it to do its job; but also checks and balances that required it to act proportionately and reasonably.

We believe that government should consider tried and tested models of oversight, that includes the input of subject-matter experts from industry. In keeping with its desire to encourage innovation, and maintain meaningful protections for free expression and ensure that regulation is up-to-date and effective, the government also should consider solutions where the desired outcomes are managed through self-regulation or co-regulation, with the participation of experts in the industry. This should be informed by European and international digital accountability and co-operation models, as well as the UK's experience in other content heavy industries such as advertising.

Question 10a: If your answer to question 10 is (ii), which body or bodies should it be?

N/A

Question 11: A new or existing regulator is intended to be cost neutral: on what basis should any funding contributions from industry be determined?

IA notes the government intends for the regulator to be cost neutral to the public sector. While it is fairly normal practice for the cost of establishing and running a regulator to be recovered from industry, IA would be concerned if any industry levy went beyond the purpose of cost-recovery for the regulator, or if any regulator was reliant on income from financial penalties to fund its activities.

In addition, we believe it is important to consider the wider impacts of any new industry levy. In particular, the risk that new costs may have the effect of displacing existing industry spend on industry safety initiatives, and the risk that new costs may push smaller companies out of the market or hinder larger companies from continuing to grow.

IA also encourages the government to think holistically about new direct and indirect costs imposed on industry to ensure that various discrete costs (for example, regulator levy, Digital Services Tax, voluntary industry contributions to tackle harms), which are being considered in isolation, do not amount to an unreasonable burden when looked at cumulatively.

Question 12: Should the regulator be empowered to i) disrupt business activities, or ii) undertake ISP blocking, or iii) implement a regime for senior management liability? What, if any, further powers should be available to the regulator?

IA is concerned that the enforcement regime set out Section 6 is disproportionate and will have a chilling effect on internet innovation and freedom of expression in the UK. As with any regulation, there of course needs to be the threat of sanctions to act as a deterrent, but we are concerned that the OHWP proposals go well beyond what is necessary to ensure compliance.

As the government notes, the proposed powers in Paragraph 6.4 of the OHWP (i.e. civil fines, requiring remedial action, requiring information, naming and shaming) are fairly standard across regulated industries. However, we believe the thresholds for taking these actions (in particular issuing fines or naming and shaming), as well as the financial value of the penalties (with respect to civil fines) need to be more clearly defined. For example, we would only expect fines to be issued in the most serious cases of non-compliance, and we would expect there to be reasonable limits on the level of fines that could be imposed.

The government also consults on further, more novel enforcement powers, such as “disruption of business activities”, ISP blocking, and senior management liability. IA is concerned that these powers are disproportionate and inappropriate. In particular, senior management liability, combined with the extensive “duty of care” obligations, would have the practical impact of discouraging UK companies from launching internet businesses, and discouraging global internet companies from establishing operations in the UK. It would also provide a disincentive for existing businesses to continue to provide their services in the UK, which would be detrimental to people who use and enjoy a wide range of internet services.

Question 13: Should the regulator have the power to require a company based outside the UK and EEA to appoint a nominated representative in the UK or EEA in certain circumstances?

IA welcomes the government's ambition to "create a level playing field" so that companies with a presence in the UK are not disproportionately penalised – it is important that international companies with users in the UK are compliant with any regulatory regime.

That said, requiring companies based outside the UK and EEA to appoint a nominated representative in the UK or EEA risks discouraging starts-ups and small businesses from doing business in the UK, or encouraging companies to shut down existing operations. IA believes that other measures that pose fewer risks to innovation should be sought in view of holding international companies accountable for their actions.

Question 14: In addition to judicial review should there be a statutory mechanism for companies to appeal against a decision of the regulator, as exists in relation to Ofcom under sections 192-196 of the Communications Act 2003?

IA believes that companies should have a statutory right to appeal against a regulatory decision. In addition, for smaller companies in particular it is important that there is an opportunity for companies to appeal without having to go to court, as the expense and difficulty of this would provide a barrier to exercising their ability to appeal.

Question 14a: If your answer to question 14 is 'yes', in what circumstances should companies be able to use this statutory mechanism?

IA believes that companies should be able to use their statutory mechanism of appeal where there are concerns in a range of circumstances, including concerns about errors of fact, concerns about errors of law, or concerns about the exercise of the regulator's discretion.

Question 14b: If your answer to question 14 is 'yes', should the appeal be decided on the basis of the principles that would be applied on an application for judicial review or on the merits of the case?

IA believes that appeals should be decided on the merits of the case.

Question 15: What are the greatest opportunities and barriers for (i) innovation and (ii) adoption of safety technologies by UK organisations, and what role should government play in addressing these?

IA believes that there is a role for government to encourage industry to innovate in this area. However, we do not believe that government should seek to choose particular technological solutions and standards to be followed, as these are decisions which should be left to industry in order to determine the most effective solution. We would be concerned if the government attempted to mandate any particular technology or solution for all of industry to adopt.

Question 16: What, if any, are the most significant areas in which organisations need practical guidance to build products that are safe by design?

IA believes that smaller and younger companies may benefit from a general good practice guide to both safety by design and privacy by design principles. To this end, industry could work with the regulator to create non-binding good practice guides.

Question 17: Should the government be doing more to help people manage their own and their children's online safety and, if so, what?

IA supports the OHWP's general ambition for the role of digital literacy in improving online interactions, as set out in Section 9. In particular, the proposal for a new online media literacy strategy is welcome and will ideally not only help people develop the skills to safely navigate the online word, but will also increase digital civility and make it clear to people that the required standards of behaviour offline also apply online.

On the question of whether government should be doing more, at the same time as addressing online safety, we believe that we should collectively focus on addressing harms holistically – tackling societal problems both at their root in the real world, as well as in their online manifestation. We believe that a broader policy approach, looking both offline and online, will lead to better outcomes for society.

Question 18: What, if any, role should the regulator have in relation to education and awareness activity?

IA believes that any regulator should have a statutory role to promote online media literacy, in a similar way to Ofcom's current media literacy duty, for example.

Internet Association
28 June 2019