CONFIDENTIAL

Written evidence submitted by Sky (OSB0165)

Introduction

As a family brand in over 12 million UK homes, and more than 37 million homes across Europe, Sky places huge importance on the safety of our customers and their children. For many years we have played our part in keeping people safe online and this is a priority across our business:

- As an ISP Sky has led the way in providing our customers with highly customisable parental control filters to help keep their families safe online.

- As a broadcaster and content producer Sky is trusted to provide content to customers of all ages in such a way that is mindful of the needs and sensitivities of different groups.

- Sky also has a significant presence on both the buy side and the sell side of the UK advertising value chain and has numerous safeguards in place to protect consumers.

We therefore welcome the Government's ambition for a ground-breaking "coherent, single regulatory framework" for online platforms. The self-regulation of online platforms has demonstrably failed to effectively protect users from online harms and, as such, a regulatory framework is needed to support platforms in implementing and assessing safeguards.

This Bill has been the result of years of constructive debate and cooperation, which Sky is proud to have contributed significantly to. The UK has led the way in creating online safety regulation, with the Government putting the principle of proportionality into action and seeking to set a global example in striking the right balance between safety and freedom of speech.

We are broadly supportive of the regulatory approach set out by Government which is centred on a statutory duty of care and a form of 'procedural accountability'. Under the proposed system, success would be measured based on the efficacy of safeguarding systems put in place by platforms, rather than seeking to penalise companies for the occurrence of individual pieces of harmful content.

There are, however, several elements of the Draft Bill that are inconsistent with the Government's ambition to make the UK the safest place to be online – specifically the explicit *exclusion* of online consumer harms such as fraud, intellectual property infringement, and misleading paid for advertising. Under the status quo, users are not adequately safeguarded from these harms, and as such their exclusion represents a significant missed opportunity.

There is a simple change which could rectify this – we suggest that the Online Safety Bill be amended to remove Clause 41 (6), which excludes online consumer harms from scope, and Clause 39 (2), which excludes paid for advertising from scope. Removal of these clauses does not *compel* policymakers to include these harms in the new framework – the structure of the Draft Bill requires that secondary legislation is laid for any harm to be incorporated by Ofcom into the regime. But as drafted the clauses prevent these harms *ever* being addressed by this new framework, which would appear to needlessly tie Government's hands.

Furthermore, there are several areas where further detail, or more refined language, will be needed to ensure platforms and other services in scope of the regime have the guidance necessary to act with confidence and achieve the desired regulatory outcomes. These include clauses in the draft Bill pertaining to journalism and democratically important content, enforcement measures and harmful content in scope.

Finally, in order to ensure the smooth functioning of the regime, Ofcom must be empowered with sufficient resource to be able to effectively oversee the activities of the breadth of companies in scope and to support these companies on their evolving path to compliance. Ofcom should draw upon its own experiences in regulating the broadcast and telecoms sectors as well as existing expertise from other regulatory bodies, both in the UK and internationally, to support its regulatory approach.

The Online Safety Bill has been a long time in the making and it would be a significant missed opportunity if the regulation is drawn so narrowly as to exclude certain key harms or online entities from scope. Care must be taken to ensure that the legislation and supporting guidance are future-proofed and unambiguous to facilitate the long-term success of the regime.

Online Consumer Harms

Online consumer harms – which include scams, the sale of fake and dangerous goods and services and the circulation of malware, often through pirated content – are increasingly prevalent in the UK. These illegal activities have a destructive impact that goes beyond the direct debilitating effect on victims - indeed they are linked to a cascade of harms via the activities funded by the associated proceeds.

As currently drafted, Clause 41 (6) precludes online consumer harms from ever being addressed as part of the Online Safety regime. The exclusion of these harms on the face of the legislation stands in contrast to the Government's stated ambition of a "coherent, single regulatory framework" for online platforms and raises questions about the extent to which the legislation is future-proofed. Under the regime, Ofcom will already be

equipped to comprehensively assess the efficacy of safety measures put in place by online platforms and so the Bill represents a logical vehicle for addressing the role platforms have to play in tackling online consumer harms. It would be a missed opportunity to prevent the scope of the Bill from ever being expanded in this area and, as such, **Clause 41 (6) should be removed from the Bill.**

The scale of online consumer harms in the UK is growing, with existing initiatives failing to effectively curb their occurrence

Even though the majority of online consumer harms are illegal in the UK, they are not effectively managed by existing legislation and online platforms continue to act as a vector for these harms. This is exemplified by the fact that the number of reported scams increased by 66% in the UK in the early part of 2020[1], with 2m UK adults falling victim to an online scam in the first six months after lockdown began in 2020.[2] In this context bad actors have preyed on many people's increased vulnerability, combined with increased time spent online, to devastating effect. However, this was not a pandemic related anomaly - rather it can be seen as part of a broader upward trend of increasing online fraud in the UK. Between 2010 and 2020, online fraud increased by 179%, with more than 12% of Brits impacted.[3]

Existing initiatives and legislation aimed at combating fraud, counterfeit and unsafe goods and services and IP infringement have not prevented these harms from proliferating. These initiatives fail to tackle the central role that online platforms play in both facilitating the spread of these harms and their prevention. Perpetrators of these harms regularly use online platforms as a tool to target large numbers of victims at once, often posing as legitimate users or companies. This is often carried out through paid for advertising as well as links to fake or cloned websites. Under the status quo, cybercriminals continue to act across online platforms with little fear of repercussions. Online platforms typically have terms and conditions related to these harms., However, their increased prevalence indicates that platforms are failing to effectively enforce their own policies.

Online consumer harms can affect anyone, having a devastating impact on their direct victims

Anyone can be the victim of online consumer harms and while there is no typical victim, vulnerable people are disproportionately targeted. There is

[1] 'Highest ever year for Scams in 2020', Barclays, February 2021 (https://home.barclays/news/press-releases/2021/02/highest-ever-year-for-scams-in-2020/)
[2] 'Government must add scams to Online Harms Bill – as charity warns vulnerable people are being left as 'easy prey' for scammers', Money & Mental Health, December 2020 (https://www.moneyandmentalhealth.org/press-release/vulnerable-people-online-scams/)
[3] 'Fraud online report', Uswitch, April 2021 (https://www.uswitch.com/broadband/online-fraud-report/)

often a clear and immediate financial detriment. Indeed, between April 2020 and March 2021 more than £2.3bn was lost by victims of scams in the UK.[4] In addition to this, there are often significant, and sometimes long-term, mental and physical health concerns stemming from these kinds of online harms.

Beyond the impact that online consumer harms can have on self-esteem and confidence in carrying out essential activities online, they are often linked to anxiety and depression and, particularly in the case of unsafe goods and services, physical injuries. This is illustrated by research carried out by Money and Mental Health which found that 42% people who had fallen victim to online scams felt that they had experienced a major negative impact on their mental health.[5]

The proceeds from online consumer harms, such as IP infringement, often fund other criminal activities

The perpetrators of online consumer harms have also been shown to often have connections to organised crime, with the proceeds from these harms contributing to broader illegalities. In this context, online consumer harms can cause a cascade of negative impacts, affecting not just the direct victim but also precipitating wider societal harms.

IP infringement is an example of a harm which can have serious impacts on both individuals and society at large. Illegal streaming and downloading of pirated content carry the risk of malware, scam subscriptions and extreme content, and illegal streaming services are often operated by criminal organisations which have links to other crimes.

There are two main 'accepted' business models when it comes to online IP infringement at scale:

1. **Ad-funded** – these sites typically provide free illegal access to pay TV content, such as live sports, movies and entertainment shows. Adverts appearing on these sites are very often 'bottom feeder' ads. Many are extreme in nature, with strong violence and pornography often appearing without warning, causing significant harm to young people and other vulnerable groups who use these sites. These 'free' sites can also aim to monetise their content through scam advertising, or through increasingly sophisticated forms of malware. Recent research conducted by cyber resilience experts Webroot discovered that, of the free, illegal streaming sites analysed, 92% contained some form of

[4] 'Scams rocket by 33% during pandemic', Which?, July 2021 (https://www.which.co.uk/news/2021/07/scams-rocket-by-33-during-pandemic/)
[5] 'The Queen's Speech: a missed opportunity to stop online scams', Money and Mental Health, May 2021 (https://www.moneyandmentalhealth.org/queens-speech-online-scams/)

malicious content.[6] Research has consistently shown that as many as 50% of those regularly illegally streaming have been the victims of fraud or hacking as a result.[7]

2. **Subscription-funded** – here consumers are encouraged to hand over their personal information and banking details to organised criminals. We know from recent European-wide law enforcement action that digital IP infringement is a multi-billion pound enterprise that funds other types of crime. In June 2020, the Spanish National Police dismantled a criminal network supplying IPTV to an estimated two million customers across Europe, Asia and the Middle East, worth €15 million a year in profit.[8] In 2019, a joint Europol and EU Intellectual Property Office (EUIPO) study confirmed that IP crime is increasingly carried out by sophisticated organised crime networks, posing a growing national security threat across Europe.[9]

The links between piracy-related harms and online platforms are clear. A considerable number of people who come to IP infringement or piracy for the first time do so via online platforms, with 63% accessing such content via Google, Facebook or WhatsApp.[10] Despite lengthy policy processes aimed at addressing these issues on a voluntary basis, IP infringement on online platforms continues to be widespread with enforcement action remaining extremely difficult to pursue.

The Online Safety Bill should not exclude consumer harms from scope

The Online Safety Bill provides a logical vehicle for the Government to address online consumer harms, with specific reference to the role online platforms have to play in tackling these illegal online activities; however, the majority of online consumer harms are explicitly excluded from scope on the face of the Bill by virtue of Clause 41 (6). Although many illegal activities are not explicitly covered in the Online Safety Bill, the inclusion of this clause precludes these specific harms from *ever* being addressed by the new framework.

---

[6] 'We explored the dangers of pirated sport streams so you don't have to', Webroot, May 2021 (https://www.webroot.com/blog/2021/05/12/we-explored-the-dangers-of-pirated-sport-streams-so-you-dont-have-to/)

[7] 'Infringement Tracker', Industry Trust for IP Awareness, Q2 2020

[8] 'Illegal streaming service with over 2 million subscribers worldwide switched off', Europol, June 2020 (https://www.europol.europa.eu/newsroom/news/illegal-streaming-service-over-2-million-subscribers-worldwide-switched)

[9] 'Intellectual property crime threat assessment 2019', EUIPO and Europol, June 2019 (https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2019_IP_Crime_Threat_Assessment_Report/2019_IP_Crime_Threat_Assessment_Report.pdf)

[10] Sky Annual Content Privacy Survey, produced by Redblue, 2020

The rationale for actively excluding these harms is weak. These harms are not effectively managed by existing legislation and they can be equally as psychologically damaging as harms in scope of the regime as well as entailing additional financial and physical risks. When perpetuated via online platforms, significant numbers of people can be impacted, with bad actors targeting large groups of potential victims. Many of these harms are also carried out by individual users and, as such, cannot reasonably be excluded on the basis of a focus on 'user-generated' harms. Ofcom has established statutory duties to both citizens and consumers, but the new regime does not make adequate provision for its regulatory role in consumer protection.

If the Online Safety Bill is to achieve the Government's aim of making the UK the safest place to be online, and act as a "coherent, single regulatory framework" for online platforms, it must include the ability for platforms to be made accountable for tackling consumer harms. For other forms of illegal activity, the Online Safety Bill gives the Secretary of State the power to identify and target specific harms and gives Ofcom the power to set minimum standards for platforms to address these harms, and to scrutinise the effectiveness of each platform's approach. The same approach should apply to online consumer harms.

It is vital that the Online Safety Bill is amended to remove Clause 41 (6) and to leave the door open to including these harms in the scope of the regime. This would enable the Government and Ofcom to assess whether these harms were being adequately addressed elsewhere and whether they should be included in scope, with the provision for secondary legislation enabling the regime to adapt to evolving harms and technologies. In the interim, **the Government should set out clearly how it intends to mitigate consumer harms perpetrated via online platforms**, to limit the number of people adversely affected

Online Advertising

Online advertising and online consumer harms are closely linked, with bad actors often using paid for advertising on online platforms to target large numbers of users. These adverts may be for dangerous services carried out by unlicensed practitioners, goods that, once purchased, will never be sent, fraudulent investment opportunities, or any number of other harmful and illegal enterprises. In addition to consumer harms, paid for online advertising can be used to spread dangerous disinformation or links to cloned or misleading websites.

As it stands, online platforms profit from hosting these adverts, and, as such, should take responsibility for the associated harmful content which they disseminate. Whilst the majority of online platforms have a policy for moderating adverts which appear on their services, recent polling conducted

by Money and Mental Health found that over half of people in the UK see scam adverts online at least once a month.[11] This indicates that the current safeguards put in place by online platforms are ineffective; however, under the status quo, platforms are not adequately held to account for the rigour of their standards.

Furthermore, existing regulations in this area have proven to be lacking when it comes to tackling fraudulent online advertising, with the FCA itself acknowledging that it has limited power to take down such advertising.[12] Likewise, the Charter Against Fraud has failed to prevent large scale online fraud taking place. The Online Safety framework would be an effective additional tool in the arsenal of regulators in combatting fraudulent and otherwise harmful paid for advertising and, as such, it is disappointing that Clause 39 (2) actively excludes such advertising from the scope of the Bill.

In excluding paid for advertising from the scope of the Bill, the Government may be inadvertently creating incentives for bad actors to pay for advertising to perpetuate scams and other illegal activities. Whilst the Bill contains provisions for fraudulent user-generated scams, such as fake investment opportunities, there are no provisions to stop criminals from spending relatively small amounts of money to promote this same content. This is particularly concerning given many people are unable to confidently distinguish between adverts and user generated posts on social media.[13]

The Government has stated that DCMS will consult on advertising regulation and that the Home Office will produce a fraud action plan; however, this will further delay the implementation of an effective oversight regime for online advertising, leaving more people vulnerable to scam advertisements. In line with the FCA's recommendations, meaningful change could be enacted swiftly through the incorporation of advertising safeguarding obligations on online platforms as part of the Online Safety Bill. The first step towards this is the **removal of Clause 39 (2) which specifically excludes this form of advertising from the scope of the Bill.**

The broadcast industry has demonstrated that harms connected to paid for advertising can be effectively managed. There are robust rules in place which ensure that the statutory environment for TV advertising in the UK is the

[11] 'Safety first: Why the Online Safety Bill should tackle scam adverts', Money & Mental Health, July 2021 (https://www.moneyandmentalhealth.org/wp-content/uploads/2021/06/Safety-first_-Why-the-online-safety-bill-should-tackle-scam-adverts.pdf)

[12] 'Continued failure to act against online scams highlights Government's ambivalence to major source of harm', Work & Pensions Select Committee, July 2021 (https://committees.parliament.uk/committee/164/work-and-pensions-committee/news/156360/continued-failure-to-act-against-online-scams-highlights-governments-ambivalence-to-major-source-of-harm/)

[13] 'Research on the Labelling of Influencer Advertising - Report for the Advertising Standards Authority', Ipsos Mori, September 2019 (https://www.ipsos.com/sites/default/files/ct/news/documents/2019-09/asa-online-ad-labelling-report.pdf)

most stringent across all media. By contrast, whilst global online platforms compete with UK broadcasters for advertising revenue, they currently have no regulatory obligations (beyond the general law) in relation to consumer or child protection in online advertising. Online advertising remains subject to a very different regime to that of broadcast advertising with more limited rules and responsibility on the advertiser rather than the media channel.

A level playing field is needed between the regulation of broadcast advertising and online advertising, with platforms taking greater responsibility for the advertising they profit from to ensure they are themselves compliant with the advertising rules (including the protection of minors), as broadcasters currently do. Without urgent regulation, online advertising risks being the least safe segment of the internet.

Table 1: Differences in TV and online advertising regulation

Form of regulation	Television advertising	Online video advertising
Responsibility	The broadcaster who holds a television licence from Ofcom	The advertiser and not the platform
Content regulation (the context around where advertising is placed)	Ofcom Broadcasting Code	None
Advertising standards	Broadcast Committee of Advertising Practice Code – Co-regulation with backstop enforcement powers - Ofcom	Non broadcast advertising code
Pre-clearance	Clearcast clears all broadcast ads	None
Watersheds	9pm watershed for content not suitable for children	None
Amount of advertising	Minutes limited per clock hour	No limit
Product placement	Detailed rules about the due prominence of products and banned in children's programmes	No rules
Measurement	BARB panel to measure TV viewing	No commonly accepted standard

Content in Scope

The Bill provides a good outline of how the new regime will function; however, there are a number of regulatory elements that are lacking in detail. One such area of concern is the provisions around 'legal but harmful' content. Much of the language around how platforms should address this kind of content is ambiguous. This is exemplified by the fact that platforms are asked to specify how content which is harmful to adults will be 'dealt with' – a phrase which is open to interpretation and which stands in distinction to the clear obligations for platforms to take steps to mitigate and effectively manage illegal content and that which is harmful to children.

There is additional ambiguity around the threshold at which content is considered to be harmful. The draft Bill states that this is content which causes significant psychological or physical harm to an adult of 'ordinary sensibilities'; however, it is unclear what this would mean in practice. The Explanatory Note for the Bill states that the impacts on a child of ordinary sensibilities could by physical or mental, including "feelings such as serious anxiety and fear; longer-term conditions such as depression and stress; and medically recognised mental illnesses". The guidance for adults is, however, missing this level of detail. It will be vital that the bar for intervention is not set too high as this will leave users unprotected.

In defining thresholds for intervention, the cumulative impact of high volumes of lower-risk content must be considered. For example, a single instance of misogynistic content may fail to meet the threshold of harm for an adult of 'ordinary sensibilities' but if the design of a certain platform facilitates the inundation of a user with such content the harm may be grave.

More detailed guidance is also needed to advise the handing of mis- and disinformation. This type of content is not included on the face of the Bill, despite the Government's previously stated intention to include it in the scope of the regime on the basis that it is vital to protecting a healthy democracy.

Clear obligations and expectations around legal but harmful content must be set to enable platforms to effectively safeguard users. Furthermore, there does not appear to be any obligation for search engines to address legal but harmful content. This is a significant gap which should be addressed.

Journalism and Democratic Content

It is right that there are specific carve outs for legitimate journalistic content, trusted news sources and democratically important content. In Clause 39 the Government commits to ensuring that trusted news sources, such as Sky News, are clearly defined so they are not grouped with potentially contentious or illegitimate news outlets. In Clause 14, the Government also commits to building protections into the regime to ensure that legitimate news is not impacted by any measures that online platforms introduce to remove harmful content and that democratically important content is safeguarded.

While these safeguards are welcome, **it will be essential that the expectations associated with Clauses 39 and 14 are clearly defined** to give certainty to both online platforms and news media about the remit of the regime. Clarity around these obligations will help to ensure that freedom of expression is prioritised and a plurality of views is upheld under the regime.

As envisaged by Government, Ofcom must also be empowered to take a robust approach to ensuring platforms put in place adequate protections for journalistic content. There is a significant risk that platforms may act with excessive caution in managing content and, in so doing, could remove legitimate journalism out of a fear of breaching standards.

Enforcement measures

The terminology of 'infrastructure services' used in the draft Online Safety Bill implicitly recognises that internet users increasingly access content in a myriad of different ways. Internet access is a multi-component and multi-stage capability, the delivery chain between users and content involves both user devices, their operating systems and the applications they run and the internet-located services they access. Given that ISPs may have limited levels of oversight of some of these functions, it is right that the long tail of ancillary infrastructure service providers is considered when it comes to the enactment of enforcement measures, including business disruption activities.

The architecture of the internet is rapidly changing with the increased adoption of the DNS-over-HTTPS (DoH) protocol and other similar technological changes. The advent and adoption of end-to-end encryption across all the stages of connectivity (from DNS through to HTTPS) by those access components means that an ISP's abilities to oversee and control access are significantly reduced in granularity. For this reason, the adoption of DoH can reduce the efficacy from an end user perspective of ISPs implementing court ordered blocking by effectively disintermediating ISPs from the value chain between content and end users. It allows some browsers and apps to bypass ISPs and send encrypted DNS queries using their own servers. In short, it shifts the legal and economic components of data traffic oversight from ISPs to browsers and app providers.

As a UK ISP, Sky has both legal and ethical obligations to protect customers from dangerous content and applications on the internet. These obligations will be enhanced by the new Online Safety regime. Sky's blocking and filtering is currently fulfilled through a number of methods, including active inspection and modification of customer network traffic through DNS. The implementation of DoH undermines our ability to do this from an end user perspective.

As such, it is right that the Government ensure responsibilities for blocking is shared across the internet value chain to ensure the effective functioning of the regime. Additionally, **in its role as Online Safety regulator, it will be vital that Ofcom consistently engages with key entities in the internet value chain beyond ISPs. Going forward, it will be important that the Government ensures the adoption of DoH and other similar technological developments are compatible with obligations in the Online Safety regulatory framework.**

Furthermore, court ordered blocking carried out by ISPs and other entities in the internet access delivery value chain must be a safety measure of last resort. Relying on such blocking requests to be issued is often not the best approach to tackling many kinds of harmful online content as this process can be lengthy and the longer such content remains live for, the more people are exposed to it. As such, **it will be vitally important that online platforms have effective and responsive mechanisms for addressing harmful content as it arises, without having to wait for blocking requests to be enacted.**

Regulatory framework

Ofcom is well placed to become the Online Safety regulator and Sky welcomes this appointment. The broadcast regulation framework forms a helpful basis for the online safety regime as Ofcom has already demonstrated that it can regulate harms in a proportionate manner based on context and audience, whilst maintaining diversity of content and freedom of expression. Ofcom also regulates the telecoms sector and, whilst the regime is not directly focussed on harmful content or issues of freedom of speech, it does set out requirements for how companies should respond to consumer harm. In so doing, Ofcom has demonstrated that it is able to give consideration to how different parts of the value chain can best address different types of harm.

In its role as Online Safety regulator, Ofcom should bring together elements of its regulatory approach in both broadcast and telecoms to ensure a well targeted regime. Ofcom should also be enabled to work with other regulators who have differing areas of expertise of relevance to the regime. This could be done through formal 'co-designation' of powers or through informal cooperation. The Online Safety regime will overlap with and be informed by various other frameworks which are in place or in development, including the Age Appropriate Design Code, the Video-Sharing Platforms regulation and the proposed reformed competition regime. This makes the need for regulatory cooperation and coordination pronounced.

Alongside regulatory cooperation, **Ofcom should draw on established expertise to ensure effective oversight and, given the global impact of online safety issues and the global footprint of many large online platforms, Ofcom should seek to share insights with other international regulatory bodies.**

In order to ensure the smooth functioning of the regime, Ofcom must also be empowered with sufficient resource. This will aid Ofcom in its stated collaborative and constructive approach to regulation in which it plans to work closely with platforms to help them become compliant. It is right that the Government has taken a tiered approach to compliance based on factors

including size, demographic of user base and business model. This should prevent the regime from placing a disproportionate regulatory burden on SMEs or low risk entities.

Under the proposed regime, online platforms will have significant freedom to design safeguarding approaches that are best suited to their business models and the demographics of their users, and to assess the efficacy of these measures. As part of this, platforms will carry out their own risk assessments. Ofcom is due to publish guidance for platforms on risk assessments, although this will be non-binding and there does not appear to be a mechanism for Ofcom to challenge the validity of individual risk assessments.

In this context, it is particularly important that platforms use all the tools available to them to accurately assess who is using their platforms. Under these obligations, companies will have to assess whether children can access their service and whether this is likely. **Robust age verification mechanisms could play an important role in enabling platforms to assess the age demographic of their users with confidence.**

Conclusion and recommendations

An effective and comprehensive online safety legislative framework is urgently needed in the UK. The lack of a clear regime in place for tackling online harms has meant that bad actors have been able to exploit people's vulnerabilities at scale during the COVID-19 pandemic, with instances of many forms of online harm, particularly online consumer harms increasing significantly during this period. Many of those perpetuating online abuse and exploitation have done so with little fear of repercussions, even in cases of illegal activity.

In this context, it is right that the Government seeks to refine the Online Safety Bill and get the regime up and running as soon as possible; however, the speed of commencement should not be prioritised at the expense of getting the Bill right. The Online Safety Bill represents a unique opportunity to address a wide spectrum of online harms in a coherent manner, drawing on the established expertise of Ofcom and other regulators and addressing gaps in existing initiatives.

It would be missed opportunity to draw the scope of the regime so narrowly as to prevent online harms from being addressed in a comprehensive manner and to necessitate parallel legislation to be drawn up in the near future, risking confusion and the creation of compliance conflicts. Furthermore, it would be short sighted to fail to address ambiguities in the language of the Bill and supporting guidance in an effort to secure the hasty commencement of the regime. For these reasons, Sky proposes the following recommendations which are targeted at ensuring the obligations in the Bill

are clear for all parties and the Government achieves its aim of making the UK the safest place to be online.

- The Online Safety Bill should be amended to remove Clause 41 (6) which prohibits the inclusion of online consumer harms in the scope of the regime. The Government should consider addressing these harms as part of the wider online safety framework and, in the interim, set out clearly how it intends to mitigate consumer harms perpetrated via online platforms.

- The Online Safety Bill should be amended to remove Clause 39 (2) which prohibits the inclusion of paid for advertising from the scope of the regime. The Government should consider addressing paid for advertising as part of the wider online safety framework.

- Clearer obligations and expectations around the thresholds for legal but harmful content must be set to enable platforms to effectively safeguard users. In defining thresholds for intervention, the cumulative impact of high volumes of lower-risk content must be considered.

- The Bill should be amended to include an obligation for search engines to address legal but harmful content.

- Guidance should be issued on the handling of mis- and disinformation as part of the regime.

- Online platforms should be encouraged to put in place robust age verification mechanisms to assess the age demographic of their users with confidence.

- Clear expectations should be established regarding the protections for journalistic and democratically important content set out in Clauses 39 and 14.

- Guidance should be issued regarding additional obligations for online platforms to ensure that those closely involved with democratic processes, such as elected officials and journalists, are adequately protected from harmful content.

- When seeking to implement enforcement activities, Ofcom must engage with entities across the internet value chain, in addition to ISPs, taking into account the impact of technical changes to internet architecture. In line with this, the Government should seek to ensure that the adoption of DNS-over-HTTPS and other similar technological

developments are compatible with obligations under the Online Safety regime.

- Ofcom should be empowered to work with other regulators, both in the UK and internationally, to share insights and expertise related to the Online Safety regime.

Sky September 2021

28 September 2021

26 October 2021