Written evidence submitted by TalkTalk (OSB0200)

September 2021

Introduction

TalkTalk is pleased to respond to this consultation and to see the publication of the draft Online Safety Bill. This publication comes after considerable policy deliberation and debate, which is to be expected on an issue as complex and sensitive as mitigating online harm and when developing a new regulatory and legislative framework. We congratulate the Department of Digital, Culture, Media and Sport for this significant achievement.

Our response is brief; as we are not in scope of the regulation, we do not make extensive comments on the proposed operation of the Codes of Practice and the relationship between regulated companies and Ofcom. We focus on what the draft Bill means for TalkTalk and areas where, based on our experience, we think it could be amended and/or improved.

The Bill is a complex piece of legislation to introduce novel regulation and there is no clear precedent, either within the UK or internationally. Essential to its success is that it establishes public confidence in the new regime. We know that the public, including our customers, are concerned about the prevalence of illegal and/or abusive content on social media platforms. Ofcom research in June 2021 found that 76% of people say they have been exposed to at least one potential harm online over the previous four weeks.[1]

The introduction of this Bill is a response to this public concern and the failure of a purely self-regulatory approach. Therefore, public confidence – in addition to business response – is a key test for the new regime and must be a guiding principle for the legislation.

This principle has shaped our response and highlighted two concerns regarding omissions to the legislations.

1. Firstly, the absence of economic harms, such as scams or fraudulent activity, from the legislation;
2. and, secondly, the role of other internet players apart from social media companies and ISPs.

We acknowledge there is no simple answer to these issues, nor is it necessarily clear how they could be added to the current Bill. However, we believe these issues should be explored in the scrutiny process led by Parliament, and we make recommendations about

[1] Ofcom, Online Nation 2021, June 2021

amendments at this stage so that Members can scrutinise the proposals and, if needed, make recommendations about how the regulation may need to be expanded in future.

In addition, we make some wider observations about the Bill based on our experience to date, particularly with regards to our current work on online safety and our current work with Ofcom.

TalkTalk's position

TalkTalk strongly supports the introduction of the Bill and a new regulatory structure regarding user-generated content. As discussed above, the rationale for Government action is well-established and there is strong public support for action in this area. After a long process, the proposals in the Bill are to be welcomed. DCMS and the Home Office have carefully balanced the need to tackle online harms while protecting freedom of expression and privacy rights:

- The Bill proposes a regulatory system which takes a risk-based, proportionate approach to tackling harm, prioritising the most significant platforms and the most significant harms over lesser harms.
- The proposed regulatory structure is based on well-established principles: the creation of codes of practice and the requirement to demonstrate compliance against these guides is in keeping with Ofcom's approach to regulation at the moment.
- The principles-based regulation future-proofs the regime: it will avoid overly prescriptive regulation, which risks becoming outdated, and instead empowers regulated companies with flexibility where needed to adapt to their particular business model, but ensure enough rigour to give users confidence in the processes.
- In particular, this approach enables the regime to evolve over time, rather that setting prescriptive approaches in response to particular concerns. This approach is vital if the regime is to adapt to emerging harms and new technologies- and this ability to stay relevant will be essential to its success. Ofcom, and companies, will need to be nimble and forward-looking, and the approach set out in legislation should help establish that culture.

TalkTalk's role in the regulation

TalkTalk will not be in scope of the new regulatory regime as we do not host user-generated content (with the exception of our help pages, which are very unlikely to be considered Category 1 provider). Therefore, we do not have extensive comments to make regarding the processes of the regulator and the regulator- regulated entity relationship.

Like other ISPs, we expect to play a role in Ofcom's enforcement regime as we will be required to block access to non-compliant sites. We accept this role but, in discussions with DCMS prior to publication, we called for certain conditions to be met. We are pleased that the Government listened to our views on how this process should work:

- We welcome the clear inclusion within the Bill, as this establishes a clear legal obligation for ISPs to comply with blocking requests without fear of violating net neutrality regulation.
- We welcome the involvement of the legal process by requiring a judge's approval for site-blocking requests.
- We also welcome the proposal that Ofcom will publish guidance on how Ofcom's powers in this respect will be exercised. We expect that these proposals will be subject to industry consultation prior to final publication.
- We also expect the guidance will state that site-blocking is a last resort measure, in recognition of the risk to freedom of expression from a heavy-handed approach to site-blocking.

It is also encouraging to see these provisions applied not just to ISPs, but to other parts of the internet ecosystem - for example browser providers (Google Chrome, Mozilla), app stores (Google Play, Apple App Store) and operating system providers (e.g. Apple iOS/macOS, Google Android and Microsoft Windows etc.). This is an important recognition of the changing internet landscape and is both fairer (in sharing responsibilities across the value chain) and more effective. The current move to new standards and internet protocols such as DNS over HTTPS (DoH) mean that relying on ISP blocking via DNS (which is the technology which underpins our filtering products and also the proposed way to enact the age verification regime contained within the Digital Economy Act 2016) will be less effective – ISPs are not able to see what site is being accessed and therefore not able to apply the relevant blocks.

At present, this concern is particularly acute with the deployment of Apple's Private Relay Network, based on the Oblivious DNS-over-HTTPS protocol (ODoH). This new service will see Apple work with third parties to allocate random IP addresses to users so that websites cannot track users based on their IP address. Neither proxy knows the user's IP address and the website they are visiting meaning that neither websites, Apple nor the content delivery network partners can track user activity based on their actual IP address. The resulting system removes an ISP's ability to have any influence over DNS and IP traffic destinations.

These new protocols prevent ISPs from making assessments of content, including whether it should be blocked under regulatory requirements. As an ISP, we are assessing how to respond to this shift and maintain our commitments to keeping our customers safe. In any case, this technological change demonstrates that ISPs can no longer be considered the only

entity which can control access to sites, and therefore it is correct that the Bill will require other parts of the ecosystem to tackle action to restrict access to content. This approach will ensure the regime will stay relevant as the technology changes – rather than responding to changes, it sets a broad obligation on those companies that have a role to play.

We are aware that it is likely that some of these providers – many of which are not based in the UK – will criticise the Government's approach here and argue that it is technologically difficult and/or not compatible with privacy rights. However, the Government's approach is correct and it should aim to keep this broad level of responsibility- it is appropriate for the Government to set expectations on companies based on UK law and social values. We discuss the issue of technological protocol changes below.

We support BT's proposed amendments to sections 93 and 94 of the Bill to strengthen the provision on other infrastructure providers. In particular, we hope to see the Bill amended to introduce a statutory right of appeal by providers of ancillary services and access facilities in respect of service restriction or access restriction orders made without notice. This right would help to appease concerns about damage to free speech due to hastily ordered blocking.

Areas not covered by the Bill

Economic Harm

There is widespread concern about the exclusion of economic harms from the regulatory regime. At TalkTalk, we share these concerns. While the Government has focused on user generated content, and acknowledge that the Government has a number of workstreams which relate to economic harm and fraud online, we are not convinced that it should be excluded from this Bill and the future regulatory regime.

Firstly, the Online Safety Bill (and the regulatory regime it will create) is intended to tackle online criminal and harmful behaviour on platforms. Scams and fraud clearly fall within this definition. The distinction between user generated content and other content is irrelevant – if any user chooses to use platforms to promote illegal activity, it should be tackled under the provision of the Bill. For example, a link to a fraudulent investment website should be subject to regulation regardless of whether it is posted by an individual or whether it is promoted via paid-for advertising. The content and the impact are the same – and therefore, logically, it should be part of the regime, and the same requirements around codes of practice, processes and intelligence sharing should apply as it would to other illegal activity online.

Secondly, this is a question of public confidence in the new regime. Online scams cause considerable consumer harm – UK Finance has found that £754m was stolen from bank customers during the first half of this year via online scams – a 30% rise on the same period in 2020.[2] Ofcom's 2020/2021 pilot online harms research found that scams/fraud/phishing were the second most experienced online harms after spam emails.[3] It is clear that the increased time spent on digital devices at home under lockdown has opened the door to scammers. With hybrid working set to continue, so should the trend. What's more, the prevalence of online scams is a key factor in digital exclusion, with consumers declining to engage with the online world due to their concerns about the proliferation of criminal and harmful behaviour: research by the Broadband Stakeholder Group in November 2020 found that people who are not online are concerned about the prevalence of scams online.[4]

Concern about this type of harm is well-established, as is the criminal nature of such harm. The creation of a new regulatory regime which would *not* tackle one of society's major concerns about online environments risks harming confidence in the new regime from the outset. Rather than settling the question of online regulation, it would lead to a continual press for expansion and revision in response to consumer concern. We note the wide-ranging concern about the absence of economic harm from the regime – from consumer groups (Which?, Money and Mental Health Institute) as well as finance groups (UK Finance) and both the Treasury Select Committee and the Work and Pensions Select Committee[3].

We are especially surprised that, not only are these harms excluded from the Bill, but it is one of the few types of harm which is explicitly excluded from the legislation- firstly, in Section 41 Clause 6 which excludes online fraud, the sale of counterfeit and unsafe goods and services and IP infringement, while Section 39 Clause 2 excludes such advertising from the scope of regulated harms. These exclusions in the primary legislation would means that the Bill would have to be amended before any extension to cover these policy areas would be permitted. This approach seems counter-intuitive both to the aims of the Bill and best practice in legislation.

We want to see Government respond to these concerns regarding the exclusion of economic harm and include it in the Bill, and then identify it as a priority harm for Ofcom to address. We do not deny that economic harms differ from many of the harms identified in the Bill, and would require certain specific approaches which may differ from other harms within scope. However, we contend that this would not be an insurmountable problem and indeed would not even be a unique problem, as the current framework will require different approaches depending on the harm in question. For example, the requirements on illegal

[2] UK Finance, Fraud – The Facts 2021, September 2021
[3] Parliament, "Online Safety Bill: Committees warn Prime Minister over lack of action on harmful paid-for scam adverts", July 2021

activity (e.g. child sexual abuse material) differ from the legal but harmful activity- yet both are contained within the same regulatory framework.

At the very least, Government should amend the bill to remove Section 41 Clause 6 and Section 39 Clause 2 to leave open the chance for Parliament to decide to extend the regime to cover these concerns in the future. The Committee will note that we have signed a letter along with other ISP partners and broadcasters on this issue, and we hope that the Committee and all Members note the strength of industry feeling on this issue.

Context of increased encryption

The text of the Bill does not refer to changes in the internet architecture and the trend towards more encrypted traffic. As the regulatory regime is focused on user generated content, this is to be expected.

However, the issue is central to the question of safety online. Removing harmful content requires platforms and other operators to assess the content and make a judgement on it, and that depends on visibility of content. As we discussed earlier, it is also central to the ability of other services to comply with business disruption measures, and the efficacy of these measures. These requirements will apply to non-UK based companies which may have a limited UK presence, while increased encryption will lessen the ability of UK-based companies to see and respond to harm. This will clearly impact the ability and willingness of companies to identify and respond to harm.

One clear example of this issue is the move to encrypted DNS (using the DNS over HTTPS protocol) by browser companies such as Google and Mozilla. This change prevents ISPs from seeing traffic on these DNS platforms, and therefore the ISP is unable to respond to the content in keeping with regulatory obligations on parental filtering (as well as other restrictions which largely impede the service to the customer).

We expect the Home Office to publish a voluntary best practice guidance for infrastructure service providers, which the White Paper response stated is separate from the online harms regime. Therefore, it is not to be considered as part of the pre-legislative process. However, it is important that Ofcom plays close attention to these trends as these technological changes will have determine the success of the regulatory regime. In addition, MPs must be aware of these issues and should consider them when scrutinising the Bill, and consider how Ofcom will monitor these issues and respond to any changes where required – for example, what the Codes of Practice will say on encryption.

We do not think these problems are insurmountable. In fact, recent experience has shown how different parts of the internet ecosystem can work collaboratively for the good of consumers. In the early days of lockdown, content providers and networks worked together to manage traffic on the network and took proactive steps to mitigate risk – for example, gaming providers moved planned new releases so as not to exacerbate demand on the network due to peak demand. This collaboration showed how providers could work together to both achieve their goals. We would like to see such a model replicated when it came to technological changes such as the introduction of DoH (which we do not oppose in principle, but which will take careful implantation and raises a number of questions.) These groups could consider the best balance between privacy concerns and tackling harmful content. It would facilitate greater discussion to build agreed timeframes, rather than see unilateral changes that – in the short-term- hinders an ISP's ability to protect its users. We hope that Ofcom could establish and lead these working groups – both to help it stay up to date on technological changes and to help shape its regulatory approach.

Wider working of the Bill

We make a number of points regarding the wider workings of the Bill to contribute to the Committee's scrutiny of the Bill.

- We support Ofcom taking on the role of online harms regulator. It has strong experience in making regulation on complex areas, particularly regarding content standards, as well as assessing the impact and trajectory of new technologies. This twin experience makes it the best placed regulator to take on this responsibility. TalkTalk is regulated by Ofcom as a broadband and telephony provider and we can speak from experience about its commitment to proportionate regulatory action.
- We recognise that this represents a considerable extension of Ofcom's remit, and comes alongside expanded powers in other areas (for example, new powers on telecoms security.) This poses operational challenges which need to be addressed so that all companies regulated by Ofcom understand how it will respond.
- We believe there is a strong case for Ofcom to co-designate other bodies to help it deliver its regulatory functions.
    - This question is particularly pertinent when it comes to the Internet Watch Foundation (IWF), a charity which works with industry to identify and remove child sexual abuse material online. The IWF has clear expertise which Ofcom should harness, rather than seek to duplicate.
    - This model could also be applicable with economic harms such as fraud and scams. While Ofcom would remain the ultimate authority and be accountable to Parliament, co-designation would enable it to draw on external advice and support as needed.

- We note that the current draft of the Bill does not contain the "co-designation" powers for OFCOM that appeared in the December policy document. We would like to see those acknowledged and made explicit in the text of the Bill.
- It is essential that Ofcom's regulatory independence is not compromised with the extension of its remit. We share concerns expressed elsewhere about the wide range of powers that the Bill awards to the Secretary of State to direct Ofcom, in particular its ability to modify Ofcom's Code of Practices and identify priority harms to be addressed. This approach risks undermining Ofcom's regulatory independence and could see its regulatory decisions drawn into a political context, which would undermine industry and public confidence in the regime. Therefore, the final bill should include more safeguards to defend Ofcom's independence.

Conclusion

To conclude, TalkTalk welcomes this Bill as a much-needed response to real harm being perpetrated online. We consider that the Government has broadly judged the balance right between freedom of expression and protection of users, although this balance will have to be constantly monitored and challenged. Our main concerns relate to the exclusion of economic harm from the scope, which we consider to be a missed opportunity. We also consider that more discussion is needed about how technological change is developed and implemented. The regulatory system will be tasked with overseeing a hugely diverse and innovative sector. Its success will be determined by how it can shape the changing technological environment – or whether it can only respond to changes after it happens. This is the key question for the Bill as it goes through Parliament.

29 September 2021