Dame Margaret Hodge MP
Member of Parliament for Barking
House of Commons, London SW1A 0AA
Tel: 020 7219 6666

Written evidence submitted by Dame Margaret Hodge MP (OSB0201)

Joint Committee on Draft Online Safety Bill
House of Lords
London
SW1A 0PW

5 October 2021

Dear the Joint Committee on Draft Online Safety Bill,

Please find enclosed my written submission, following the Call for Evidence for the Draft Online Harms Bill.

In the two months of October and November 2020, the Community Security Trust (CST), an antisemitism monitoring organisation, found there were about 90,000 mentions of my name or Twitter handle, including retweets and shares, following the Equality and Human Right's report on antisemitism in the Labour Party. It found that 22,000 individuals had been involved.[1] The abuse was often offensive in itself, but it also promoted lies about me and painted a false portrait of who I am, including that I have supported apartheid and was a paedophile. The purpose of this was to paint me as a terrible person who could not be trusted. So, if I then said any of this publicly, my views could be discounted and ignored. The platforms that were intended to enhance and strengthen democratic discourse are being used to close down voices and inhibit democratic discourse.

As a result, I have long been concerned about online safety and online harms. I have spoken in Urgent Questions to the Department of Culture, Media, and Sport regarding racist abuse on social media, participated in a Backbench Business debate on Online Anonymity and Anonymous Abuse, and in the Online Harms Consultation on antisemitic abuse. I have also written about my concerns with online anonymity in the Guardian.

My experience with online abuse, and my work on tax avoidance and financial crime, has shaped my written submission. Thus, the questions pertinent to the committee which I have prioritised in this submission include the protection of children and vulnerable adults from harmful content, the definitions of 'duty of care,' 'legal but harmful' and 'terms and conditions' in the bill, omissions within and the scope of the Online Safety Bill, and OFCOM's role in monitoring abuse.

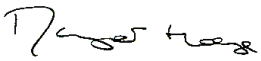
[1] Jessica Elgot (December 2020), *'Margaret Hodge calls for ban on social media anonymity,'* The Guardian, https://www.theguardian.com/society/2020/dec/06/margaret-hodge-calls-for-ban-on-social-media-anonymity

Constituency Office:
Barking Learning Centre, 2 Town Square, Barking, IG11 7NB
margarethodge@hotmail.co.uk
07707045254 or 07595970515
www.margarethodgemp.com

Dame Margaret Hodge MP
Member of Parliament for Barking
House of Commons, London SW1A 0AA
Tel: 020 7219 6666

Should you wish to publish an edited version of this document, I would be happy to provide the file in its original format. I hope these considerations are helpful in the next stage of your inquiry and am grateful for being provided the opportunity to respond.

Yours sincerely,



Dame Margaret Hodge MP

Call for evidence: Joint pre-legislative scrutiny Committee on the Draft Online Safety Bill

Written Submission by Dame Margaret Hodge MP

Introduction

Dame Margaret Hodge has been the MP for Barking and Dagenham since 1994. A member of the Labour Party, she previously served as Leader of Islington London Borough Council from 1982 to 1992. She has held a number of ministerial roles and served as Chair of the Public Accounts Committee from 2010 to 2015.

In the two months of October and November 2020, the Community Security Trust (CST),[2] an antisemitism monitoring organisation, found there were about 90,000 mentions of my name or Twitter handle, including retweets and shares, following the Equality and Human Right's report on antisemitism in the Labour Party. It found that 22,000 individuals had been involved.[3] The abuse was often offensive in itself, but it also promoted lies about me and painted a false portrait of who I am, including that I have supported apartheid and was a paedophile. The purpose of this was to paint me as a terrible or wicked person who could not be trusted. So, if I then said any of this publicly, my views could be discounted and ignored. The platforms that were intended to enhance and strengthen democratic discourse are being used to close down voices and inhabit democratic discourse.

Margaret's personal experience compiled with her work on tax justice has led her to get involved in the scrutiny of the Online Safety Bill.

Summary

[2] The Community Security Trust (CST) is a charity that protects British Jews from antisemitism and related threats. More information is available at: https://cst.org.uk/about-cst
[3] Jessica Elgot (December 2020), *'Margaret Hodge calls for ban on social media anonymity,'* The Guardian, https://www.theguardian.com/society/2020/dec/06/margaret-hodge-calls-for-ban-on-social-media-anonymity

Constituency Office:
Barking Learning Centre, 2 Town Square, Barking, IG11 7NB
margarethodge@hotmail.co.uk
07707045254 or 07595970515
www.margarethodgemp.com

Dame Margaret Hodge MP
Member of Parliament for Barking
House of Commons, London SW1A 0AA
Tel: 020 7219 6666

1. In the social media age online abuse has become a new source of oppression, with women and Black, Asian and Minority Ethnic (BAME) persons being disproportionately targeted. Amnesty International found that one in five women in the UK have suffered online abuse or harassment, and black women are 84% more likely than white women to be mentioned in abusive or problematic tweets.[4]

2. Online abuse inhibits people, in particular women and girls, from accessing relevant information, expressing their opinions and participating in public debates, acting as a further barrier to women's political participation. At the 2019 General Election, a number of prominent women MPs stood down, citing the continued abuse they received online as one of their key reasons.[5]

3. Protected minorities are more likely to experience abuse on social media, and as a result, antisemitism is a huge issue online. A large-scale study conducted by the Centre for Countering Digital Hate (CCDH) recently found that nearly nine out of ten antisemitic posts on Facebook and Twitter stay online despite being reported.[6] The CCDH collected and reported 714 posts containing anti-Jewish hate, which said it had been viewed more than 7.3 million times across Facebook, Instagram, TikTok, Twitter and YouTube.[7] According to the report, 80 per cent of posts containing Holocaust denial and 70 per cent of posts identified as neo-Nazi were not acted upon despite clearly being in breach of platform rules around hateful content.[8]

4. This shows that platforms are failing to remove hateful and antisemitic content even after it is specifically reported and flagged. Although the tech companies have levelled the argument that their algorithms allow automated hate removal, it is clear that Big Tech has failed to address the endemic within hatred that their platforms host.

5. Platforms must radically remedy their moderation systems which have been proven to be ineffective, and governments must find a way to hold platforms accountable for their failures to act. However, The Online Safety Bill (hereafter OSB),[9] while a welcome step forward, does not go far enough and has significant omissions which would ensure hatred on these platforms was stamped out.

---

[4] Amnesty International (2018), *'Women abused on Twitter every 30 seconds - new study,'* https://www.amnesty.org.uk/press-releases/women-abused-twitter-every-30-seconds-new-study
[5] Centenary Action Group (2020), *'End online abuse,'* https://www.centenaryaction.org.uk/our-campaigns/end-online-abuse
[6] Centre for Countering Digital Hate (2021), *'Failure to Protect: How tech giants fail to act on user reports of antisemitism,'* https://252f2edd-1c8b-49f5-9bb2-cb57bb47e4ba.filesusr.com/ugd/f4d9b9_cac47c87633247869bda54fb35399668.pdf
[7] Ibid.
[8] Ibid.
[9] Throughout the bill will also be referred to as the Online Harms Bill, OHB or OSB.

Constituency Office:
Barking Learning Centre, 2 Town Square, Barking, IG11 7NB
margarethodge@hotmail.co.uk
07707045254 or 07595970515
www.margarethodgemp.com

Dame Margaret Hodge MP
Member of Parliament for Barking
House of Commons, London SW1A 0AA
Tel: 020 7219 6666

Recommendations

Each of these recommendations will be addressed further in the written submission. The UK Government should tackle the following issues:

6. **The differing language between the abuse children and adults face**: the new guidelines proposed within the draft bill which addresses the removal of illegal content online focuses on three themes: child sexual abuse, terrorist material and media that promotes suicide. Furthermore, the strong new code of conduct for companies primarily sets out their responsibilities towards children. This stringent language is welcome, however, it should also be extended to the content adults view, rather than creating a gulf between some manifestation of illegal material online and other harmful content.

7. **Terms and Conditions:** while the bill allows social media platforms to set their own terms and conditions for their users, self-regulation by the platforms is evidently not working. Platforms are failing to enforce their own rules and allow their sites to become safe places to spread racism and propaganda, in particular against minority groups.[10] A minimum standard for the terms and conditions of these platforms must be set, as these platforms cannot be trusted to set stringent regulations themselves to keep all their users safe, and OFCOM must monitor the platforms and ensure they adhere to these standards.[11]

8. **Legal but harmful language:** while the OSB is addressing legal but harmful content in Category One services, such as information regarding eating disorders, and disinformation and misinformation, it must also extend these obligations to Category 2 companies. Furthermore, the definition of legal but harmful as content which "gives rise to a reasonably foreseeable risk of a significant adverse physical or psychological impact on individuals" is too ambiguous. The definition of what constitutes 'legal but harmful' language will inevitably be complex and subjective; however, this should not be a reason to avoid this issue. The ability to decide and judge what constitutes 'legal but harmful' language must be given to OFCOM. The judgements by both OFCOM and the platforms will also be subject to judicial review. Over time, an understanding of what constitutes 'legal but harmful' language will evolve.

[10] Adam Smith, *'Almost All Antisemitic Posts Stay Online Despite Being Flagged, New Social Media Report Claims,'* The Independent, https://www.independent.co.uk/life-style/gadgets-and-tech/antisemitism-social-media-facebook-twitter-youtube-tiktok-b1895089.html

[11] For more information on the failure of social media companies to self-regulate individually, see by Michael A. Cusumano, Annabelle Gawer, and David B. Yoffie (January 2021*), 'Social Media Companies Should Self-Regulate. Now,'* Harvard Business Review, https://hbr.org/2021/01/social-media-companies-should-self-regulate-now

Constituency Office:
Barking Learning Centre, 2 Town Square, Barking, IG11 7NB
margarethodge@hotmail.co.uk
07707045254 or 07595970515
www.margarethodgemp.com

Dame Margaret Hodge MP
Member of Parliament for Barking
House of Commons, London SW1A 0AA
Tel: 020 7219 6666

9. **Definition of Category One social media companies**: Category One must go beyond the 3% of major social media companies (such as Twitter and Facebook) that this category would capture, to include new start-ups.[12] Size alone should not be the only determinant factor, but 'functionality' is not necessarily enough either. The risk from platforms like 8Chan, Bitchute, and Gab is known. Therefore, the requirements imposed on Category One companies must be extended to those platforms known to ferment violent extremism. For example, those on the risk register developed and maintained by OFCOM.[13]

10. **Child safety**: Government's OSB will repeal elements of the Digital Economy Act (DEA, 2017), making OFCOM the regulator of pornographic websites for illegal content, such as child pornography, as opposed to the BBFC.[14] This is welcome. However, OFCOM must have the powers and capacity to identify and remove illegal material from websites as quickly and efficiently as possible, as the BBFC currently does. Furthermore, the issue of end-to-end encrypted messaging must be addressed, in order to ensure child grooming gangs can be traced.

11. **Address anonymous abuse:** anonymity online should be protected. However, as anonymous accounts generate the majority of the abuse and misinformation spread online, anonymous abuse must be addressed. The ability to trace the perpetrators of online abuse does entail damaging the important right that is vital to many.[15] A system of how traceability ensuring users are accountable online could work is set out in this submission.

12. **Criminal liability for Chief Executives (CEOs):** the buck must stop at the top – the chief executives of these companies must be held liable for the abuse that appears on their platform. Fining companies is an important first step, but it may well be treated as a business cost. Behaviour and responsibility are more likely to change when directors are held personally accountable.

13. **Fraud via advertising**: the bill does not extend to fraud via advertising, emails or cloned websites (financial harms), despite extending to user generated content. Although the Government has pledged to publish a Fraud Action Plan after the 2021 Spending Review and the Department for Digital, Culture, Media and Sport (DCMS) will consult on online

[12] Antisemitism Policy Trust (December 2020), *'Government's Online Harms White Paper Response,'* https://antisemitism.org.uk/wp-content/uploads/2020/12/A-prelude-to-the-online-safety-bill-December-2020-FINAL-1.pdf, p. 4.
[13] Ibid.
[14] Digital Economy Act (2017), Part 3, https://www.legislation.gov.uk/ukpga/2017/30/contents/enacted
[15] David Babbs (2019), '*New year, new internet? Why it's time to rethink anonymity on social media*,' https://inforrm.org/2020/01/31/new-year-new-internet-why-its-time-to-rethink-anonymity-on-social-media-david-babbs/

Constituency Office:
Barking Learning Centre, 2 Town Square, Barking, IG11 7NB
margarethodge@hotmail.co.uk
07707045254 or 07595970515
www.margarethodgemp.com

Dame Margaret Hodge MP
Member of Parliament for Barking
House of Commons, London SW1A 0AA
Tel: 020 7219 6666

advertising to evaluate how to tackle this issue,[16] the Online Harms Bill provides the perfect opportunity to address this, simply by extending the provisions applied to user generated content to paid-for advertisements.

14. **Newspaper websites**: Recognised news publisher comment boards are not included in the OSB regulations. The Government therefore must amend this clause to ensure existing regulators/regulated publications have powers and duties in place to address harm on relevant comment boards.

15. **OFCOM**: it makes sense for OFCOM to be the regulator for online harms. However, there are concerns that need to be addressed. The present government proposal is for only an annual transparency report from tech companies to be produced assessing their ability to remove harmful content. This is too little too late. OFCOM must have the power and resources to demand material from the platforms is sent to them straight away, not a year after the post is published, and ensure legal but harmful content is immediately removed from social media platforms, as is the case in Australia.[17] Furthermore, far more resources need to be provided to OFCOM to enable them to carry their duties out efficiently.

Written evidence

Question One: Does the draft Bill make adequate provisions for people who are more likely to experience harm online or who may be more vulnerable to exploitation?

In order to understand this, it is important to understand how this bill emerged. In April 2019, the Online Harms White Paper was published proposing that all technology companies, big or small, will have a duty of care to their users commensurate with the role those companies play in our daily lives.[18] After a period of consultation, the Government released their full response to the white paper on 15 December 2020. On 12 May 2021, the Government released the draft OSB.[19] The Bill establishes a new regulatory framework which aims to set out the responsibilities set on social media companies to keep users in the UK safer online, by imposing duties of care in relation to illegal content and *content that is*

[16] Department for Digital, Culture, Media and Sport (December 2020*), 'Online Harms White Paper: Full government response to the consultation,'* https://www.gov.uk/government/consultations/online-harms-white-paper/outcome/online-harms-white-paper-full-government-response
[17] Susanne Norris (May 2021), '*Online Harms Bill: what you need to know about new online harms laws,'* Good House Keeping, https://www.goodhousekeeping.com/uk/consumer-advice/technology/a36051531/online-harms-bill/
[18] Local Government Association (July 2021), 'Must Know: Online harms,' https://www.local.gov.uk/publications/lga-online-harms
[19] Ibid.

Constituency Office:
Barking Learning Centre, 2 Town Square, Barking, IG11 7NB
margarethodge@hotmail.co.uk
07707045254 or 07595970515
www.margarethodgemp.com

Dame Margaret Hodge MP
Member of Parliament for Barking
House of Commons, London SW1A 0AA
Tel: 020 7219 6666

harmful to children, whilst also imposing duties on providers to protect rights to freedom of expression and privacy.[20]

The key point is that the White Paper emerged following increasing concern about the abuse children face online. In its conclusion, it stated "the pandemic has underlined a much graver problem; the risks posed to children online. In a month-long period during lockdown, the Internet Watch Foundation and its partners blocked at least 8.8 million attempts by UK internet users to access videos and images of children suffering sexual abuse."[21] The White Paper and the clauses focussed primarily on the critical needs of children and their protection. This can be seen in the paper's stated intention: "[protecting] children and young people against a comprehensive range of online harms – from terrorism and racism to abuse and pornographic content."[22]

This means the Bill proposes further duties of care for children in comparison to adults. Providers of user-to-user services that are likely to be accessed by children must assess the risk that content that is harmful to children can be accessed on their service.[23] Also, The Secretary of State can designate types of content as harmful to children, but service providers also must make their own judgments about whether there are reasonable grounds to believe there is a risk of content having an adverse physical or psychological impact on children.[24] Companies are also required to keep a children's risk assessment if their services lend themselves to use by children and information about some of this will be required to be fed back to Ofcom.

While the issues facing children are of paramount importance, there are also issues facing adults that need to be addressed. The language relating to children (Clause 10) talks of 'mitigation and prevention,' in social media companies' risk assessments. However, the basic risk assessment for adults (set out in Clause 9) only includes methods to 'minimise' the presence, length of time, availability of illegal content, which must be removed 'swiftly' once made known to companies.[25]

It is cause for concern that there is a gulf between the harmful abuse adults witness (the language of "minimise abuse"), in comparison to the abuse children receive (the language of 'prevent/mitigate abuse' in clause 9/10). The bill must be consistent in its approach to

[20] Ibid.
[21] Department for Digital, Culture, Media and Sport (December 2020), *'Online Harms White Paper: Full government response to the consultation,'* https://www.gov.uk/government/consultations/online-harms-white-paper/outcome/online-harms-white-paper-full-government-response
[22] Ibid.
[23] Ibid.
[24] Ibid.
[25] Ibid.

Constituency Office:
Barking Learning Centre, 2 Town Square, Barking, IG11 7NB
margarethodge@hotmail.co.uk
07707045254 or 07595970515
www.margarethodgemp.com

Dame Margaret Hodge MP
Member of Parliament for Barking
House of Commons, London SW1A 0AA
Tel: 020 7219 6666

protecting all people from illegal behaviour. This means the language of 'mitigation and prevention' must be applied to the harmful content adults view.

1.1 Recommendation

In summary, the new guidelines proposed primarily concern the protection of children as 'vulnerable users', by prioritising the removal of illegal content such as child sexual abuse, terrorist material and media that promotes suicide, and this is particularly evident in the strong new code of conduct imposed on companies that sets out their responsibilities towards children. This stringent approach to online harms children face should also be extended to adults. Specifically:

- The language of 'minimising harm' for adults must change to 'mitigation and prevention.'
- The risk assessments required of companies accessed by children must also be required by all social media companies with a large adult usership.

Question Two: Is the "duty of care" approach in the draft Bill effective?

In line with the government's response to the Online Harms White Paper, the Bill imposes a range of statutory duties of care on regulated services providers, broadly to protect users from illegal content generated and shared by other users. The proposed duty of care imposes requirements on providers, both in terms of processes they must implement and their moderation of specific content.

Under the duty of care, the bill states social media companies will need to:

- Stop illegal information and activity.
- Send the information that is asked for by the regulator.
- Where needed, set up a way of dealing with complaints and appeals which is in line with the rules set out by the regulator.[26]

However, the OSB does essentially leave it up to platforms themselves to apply these duties of care through their own Terms and Conditions (clause 11) that they can develop themselves, so long as they are 'consistently applied.'[27] Furthermore, the bill says as long as companies create terms and conditions that specify how priority content, and any other harmful content identified in a risk assessment, will be 'dealt with' by the service, this should be enough to mitigate abuse and ensure a duty of care for its users is applied.[28]

[26] Ibid.
[27] Ibid.
[28] Ibid.

Constituency Office:
Barking Learning Centre, 2 Town Square, Barking, IG11 7NB
margarethodge@hotmail.co.uk
07707045254 or 07595970515
www.margarethodgemp.com

Dame Margaret Hodge MP
Member of Parliament for Barking
House of Commons, London SW1A 0AA
Tel: 020 7219 6666

This is cause for concern. Social media companies are unable and unwilling to regulate themselves. They cannot be trusted to develop and apply these duties of care to a high standard in their terms and conditions.[29] Journalist Steven Levy has explained this by describing how, while digital platforms can be highly profitable businesses that connect users and other market actors in ways not possible before the internet, "*this can be a double-edged sword*."[30] He has said "*when they are successful, they generate powerful feedback loops called network effects and then monetize them by selling advertisements. Yes, they have generated trillions of dollars in wealth. But this has come alongside the enabling of the distribution of fake news and fake products, manipulation of digital content for political purposes, and promotion of dangerous misinformation on elections, vaccines, and other public health matters, as this disinformation and provocative content garners more usership, and 'clicks,' thus more profit. Therefore, there is little incentive to ensure this content is removed from their platform*."[31]

Social media's ad-supported ecosystems explained above shows they do not have an incentive to control what content shows up.[32] This ad-based system means social media models are based on engagement. Facebook's 'feed' aims to drive views to increase advertisements, meaning it privileges incendiary content, setting up a stimulus–response loop that promotes outrage expression.[33] In this design, Facebook assesses dozens of factors to increase engagement, ranging from who posted the content to their frequency of posts and the average time spent on this piece of content. Posts with higher engagement scores are included and prioritized; posts with lower scores are buried or excluded altogether. The problem with such sorting, of course, is that incendiary, polarizing posts consistently achieve high engagement.[34] The more people who engage with a platform and increase their use-time, the more advertisers can monetize off this usage, meaning Facebook increases its profit.[35] In the first quarter of 2020, Facebook netted $17.4 billion in advertising.[36]

Similarly, YouTube uses a similar algorithm, which has been criticized for leading users towards more extreme content. It ensures the user will stay on the platform longer and therefore engage with more ads, as extreme content is more gripping. Across both

[29] Arisha Hatch (2021), *'Big Tech companies cannot be trusted to self-regulate,'* Tech Cruch, https://techcrunch.com/2021/03/12/big-tech-companies-cannot-be-trusted-to-self-regulate-we-need-congress-to-act/
[30] Steven Levy (2020), *Facebook: The Inside Story,* Penguin, UK, p. 627.
[31] A. Cusumano, Annabelle Gawer, and David B. Yoffie (January 2021*), 'Social Media Companies Should Self-Regulate. Now.'*
[32] Ibid.
[33] Steven Levy (2020), *Facebook: The Inside Story,* Penguin, UK, p. 627.
[34] Ibid.
[35] Ibid., p. 631.
[36] Tatyana Hopkins (June 2020), '*Social Media Companies Profiting from Misinformation*,' GW Today, https://gwtoday.gwu.edu/social-media-companies-profiting-misinformation

Dame Margaret Hodge MP
Member of Parliament for Barking
House of Commons, London SW1A 0AA
Tel: 020 7219 6666

platforms, these algorithms are central and influential to their design, and it is proving to be a productive lens for toxic communication.[37]

2019 was the sixth-deadliest year on record for extremist-related violence. Social media's algorithms play a role in the radicalization of domestic extremists.[38] A case study might help explain this. The situation in Myanmar is a good example; members of the Myanmar military embarked on a lengthy Facebook campaign disseminating anti-Rohingya propaganda. Given that Myanmar has 18 million users, fake online stories such as one that circulated in 2014, claiming that a Muslim man had raped a Buddhist woman, had severe repercussions in inciting communal hatred. Human rights groups claim that the anti-Rohingya content propagated "murders, rapes and the largest forced human migration in recent history," according to The New York Times.[39] Having commissioned an independent report, Facebook admitted in 2018 that these posts were used to "incite offline violence" in Myanmar and that they had failed to remove this content.[40] Instead of learning from this, Facebook's algorithm was able to continue unhindered. In the aftermath of George Floyd's killing, Donald Trump tweeted "when the looting starts, the shooting starts" in response to Black Lives Matter protesters clashing with the police in Minneapolis.[41] Twitter took an unprecedented step in adding a warning to the tweet, saying it violated the company's rules about glorifying violence. Facebook on the other hand, decided to keep Trump's controversial posts, including one that used the same phrase as his tweet, despite being forewarned of the impact Trump's words could have.[42]

These examples illustrate the shortcomings of the proposed legislation. At best, as the bill stands, Ofcom would look at Facebook or YouTube's 'Terms and Conditions' and check whether these are being 'applied consistently' and whether they 'deal with' hate speech. But both YouTube and Facebook argue that they already do deal with this, yet these examples of racism and hate-inspired speech on the platforms show a different story.[43] If these platforms have weak terms and conditions and there is no duty on them to remove legal but harmful content, people will not be properly protected.

---

[37] Luke Munn (2020), '*Angry by design: toxic communication and technical architectures*,' https://www.nature.com/articles/s41599-020-00550-7.pdf
[38] Jonathan A. Greenblatt (Dec 2020), 'Stepping Up to Stop Hate Online,' https://ssir.org/articles/entry/stepping_up_to_stop_hate_online#.
[39] Ibid.
[40] Ayesha Kuwari (January 2021), *'Stop Hate For Profit: The Offline Consequences Of Online Hate Speech,'* https://www.humanrightspulse.com/mastercontentblog/stop-hate-for-profit-the-offline-consequences-of-online-hate-speech
[41] Ibid.
[42] Ibid.
[43] Jake Wallis Simons (June 2021), '*EXCLUSIVE 'Hitler was an angel': YouTube hosts vile Jew hatred with millions of views,'* The JC, https://www.thejc.com/news/uk/shame-of-youtube-jew-hate-1.517411

Constituency Office:
Barking Learning Centre, 2 Town Square, Barking, IG11 7NB
margarethodge@hotmail.co.uk
07707045254 or 07595970515
www.margarethodgemp.com

Dame Margaret Hodge MP
Member of Parliament for Barking
House of Commons, London SW1A 0AA
Tel: 020 7219 6666

In a recent seminar at the London School of Economics, Katie Morris, Head of Online Harms Regulatory Framework at DCMS, addressed this concern with the 'dealt with' language. She reassured the audience that *"while the government nor Ofcom will not be telling companies how to deal with 'legal but harmful' content accessed by adults, the commercial incentives are as such that it would be very unlikely that a company would choose to [enforce weak terms and conditions] and are more likely to ensure their 'dealt with' policies are strong."*[44] However, the profit social media platforms make from hateful content means this incentive is diluted, and the risk of platforms saying they have 'dealt with' legal but harmful content, when in practice they have not, remains a core concern.

2.1 Recommendation

If the fulfilment of the duty of care will be judged on the content of the platforms' terms and conditions, it is imperative that Ofcom sets out minimum standards for these published terms and the way they are implemented. Codes of Practice must set minimum standards for both the content and presentation of published terms, or we risk recreating a regime in which companies are allowed to "mark their own homework."[45]

Question Three: Are the definitions in the draft Bill suitable for service providers to accurately identify and reduce the presence of legal but harmful content, whilst preserving the presence of legitimate content?

The answer to this question leads on from my answer to question two. The main tension in the bill is over the lack of clarity on *legal but harmful* language, meaning this content will not be adequately 'dealt with,' both in their terms and conditions and in practice. There are two considerations here. The first is platforms with user-generated content (social media) and the second is search engines. Each will be addressed in turn.

3.1 Search engines

Search engines are currently not subject to the legal but harmful duty.[46] This must be included, so any language which is legal but harmful to users can be swiftly removed.

[44] Paraphrased from London School of Economics (July 2020), '*LSE Online Safety Bill Briefing*,' https://www.youtube.com/watch?v=XKKT5PjnDPk
[45] 5Rights Foundation (2021) '*Ambitions for the Online Safety Bill,*' https://5rightsfoundation.com/uploads/Ambitions_for_the_Online_Safety_Bill.pdf
[46] Department for Digital, Culture, Media and Sport (December 2020), *'Online Harms White Paper: Full government response to the consultation,'* https://www.gov.uk/government/consultations/online-harms-white-paper/outcome/online-harms-white-paper-full-government-response

Constituency Office:
Barking Learning Centre, 2 Town Square, Barking, IG11 7NB
margarethodge@hotmail.co.uk
07707045254 or 07595970515
www.margarethodgemp.com

Dame Margaret Hodge MP
Member of Parliament for Barking
House of Commons, London SW1A 0AA
Tel: 020 7219 6666

3.2 User-generated content

On user-generated content platforms, there are three main concerns. Firstly, the language is weak. Secondly, the provision to exclude 'content of democratic importance' from legal but harmful language will create concerns. Finally, the 'legal but harmful' language only has to be addressed by Category One, not Category Two, companies. This last point will be addressed in Question Four, however, the first two concerns will be addressed now.

3.2.1 Language

Firstly, the language around 'legal but harmful' content in the bill is unclear. This is primarily because what constitutes 'harm' will not be defined until secondary legislation. However, legal but harmful online content and activity is given limitations by saying it must "give rise to a reasonably foreseeable risk of a significant adverse physical or psychological impact on individuals."[47] Content that has a "minor impact" will potentially therefore not be in the scope of regulation. The narrow definition of harm does not account for content and activity that alone may not cause significant or immediate harm, but in combination, can have a serious impact. By focusing on acute harms, the legislation fails to address risks that develop over time, often with equally damaging effects.[48]

Therefore, I am concerned that adults will continue to be exposed to a substantial amount of information that is legal but can be extremely harmful by causing psychological distress, promoting self-harm and radicalization or indoctrination into extremist and racist ideologies. There are vast numbers of antisemitic, misogynist, homophobic, far-right and Islamist extremist materials, as well as disinformation other harmful content online and it is not clear from the Bill how these would be addressed, especially when present on category two platforms.[49]

3.2.2 Content of Democratic Importance

The provisions for 'content of democratic importance', in order to preserve 'freedom of speech' further impact the regulation of legal but harmful content. In the OSB, major

[47] Ibid.
[48] 5Rights Foundation (2021) '*Ambitions for the Online Safety Bill.*'
[49] Antisemitism Policy Trust (December 2020), *'Government's Online Harms White Paper Response,'* https://antisemitism.org.uk/wp-content/uploads/2020/12/A-prelude-to-the-online-safety-bill-December-2020-FINAL-1.pdf, p. 5.

Constituency Office:
Barking Learning Centre, 2 Town Square, Barking, IG11 7NB
margarethodge@hotmail.co.uk
07707045254 or 07595970515
www.margarethodgemp.com

Dame Margaret Hodge MP
Member of Parliament for Barking
House of Commons, London SW1A 0AA
Tel: 020 7219 6666

platforms will have a duty to protect content defined as 'democratically important' in order to 'uphold democratic debate online'. This is defined broadly as content 'intended to contribute to democratic political debate in the United Kingdom'.[50] However, it is unclear how legal but harmful misogynistic, racist, antisemitic, and harmful content spread by political candidates can be regulated.

There is a line to be drawn between legitimate democratic debate and content that is discriminatory and abusive, and therefore undermines the rights of others in a democracy. The Government needs to think through this and address this issue.

HOPE Not Hate has explained this concern:

"Vague and badly defined additions about protection of 'democratic speech' and comments by Oliver Dowden, Secretary of State for Digital, Culture, Media and Sport, about defences against so-called "woke campaigners", have resulted in a draft bill that could, at best fail to fix the issues it sets out to, and at worse, actually open up a path for the re-platforming of hateful far-right extremists."[51]

The main questions that need to therefore be answered by the Government are:

- What happens if content produced by a politician or journalist is also harmful?
- What is more important in this bill – reduction of harm caused by hateful online content or protection of "democratically important" speech?
- What happens when they come into conflict?[52]

Overall, under this proposed draft, it could be the case that racist and misogynist content that is legal could be re-uploaded if the content in question was deemed to be either "democratically important" or a "live political issue".[53]

3.3 Recommendation

[50] Department for Digital, Culture, Media and Sport (December 2020), *'Online Harms White Paper: Full government response to the consultation,'* https://www.gov.uk/government/consultations/online-harms-white-paper/outcome/online-harms-white-paper-full-government-response
[51] HOPE Not Hate, 'Our Response To The Draft Online Safety Bill,' https://www.hopenothate.org.uk/2021/06/07/hope-not-hates-response-to-the-draft-online-safety-bill/
[52] Ibid.
[53] Ibid.

Constituency Office:
Barking Learning Centre, 2 Town Square, Barking, IG11 7NB
margarethodge@hotmail.co.uk
07707045254 or 07595970515
www.margarethodgemp.com

Dame Margaret Hodge MP
Member of Parliament for Barking
House of Commons, London SW1A 0AA
Tel: 020 7219 6666

- The definition of legal but harmful as content which "gives rise to a reasonably foreseeable risk of a significant adverse physical or psychological impact on individuals" is too ambiguous and must be clarified.
- The definition of 'content of democratic importance' must also be narrowed in scope.
- The definition of what constitutes 'legal but harmful' language will inevitably be subjective. However, we see this in tax law. HMRC is given subjective discretion when it decides whether someone had the intent to commit tax fraud or simply made a mistake. This discretion should be given to a third party, most likely OFCOM, to ensure social media platforms are neither impeding free speech, nor not doing enough to remove legal but harmful language.

Question Four: The draft Bill sets a threshold for services to be designated as 'Category 1' services. What threshold would be suitable for this?

The categorisation of social media companies in the OSB needs to be amended. The main cause for concern within this section is Clause 3. This says that a service will only be in scope if it has a significant number of users in the UK, if the UK is a target market, or if the service can be used in the UK by individuals and there are reasonable grounds to believe that there is a material risk of significant harm to individuals in the UK.[54]

This definition would fail to capture small services which house or inspire antisemitism.[55] Size, usership, and the use by UK citizens should not be the only determinant factors. All start-ups must fall under the scope of this bill, as it is usually the smaller platforms used by a few individuals that can foster hateful behaviour, ranging from legal but harmful language to influencing violent extremism.[56]

There are also different regulations for 'Category One' companies and 'Category Two' companies. It's probably safe to assume that Category 1 companies will include those such as Facebook, TikTok, Instagram and Twitter. However, the bill does not clarify exactly what measures may be required by smaller organisations under Category 2.[57] For example, as stated in question three, only a category 1 company must have measures in place to tackle

[54] Department for Digital, Culture, Media and Sport (December 2020), *'Online Harms White Paper: Full government response to the consultation,'* https://www.gov.uk/government/consultations/online-harms-white-paper/outcome/online-harms-white-paper-full-government-response
[55] Antisemitism Policy Trust (December 2020), *'Government's Online Harms White Paper Response,'* https://antisemitism.org.uk/wp-content/uploads/2020/12/A-prelude-to-the-online-safety-bill-December-2020-FINAL-1.pdf, p. 4.
[56] Ibid.
[57] Department for Digital, Culture, Media and Sport (December 2020), *'Online Harms White Paper: Full government response to the consultation,'* https://www.gov.uk/government/consultations/online-harms-white-paper/outcome/online-harms-white-paper-full-government-response

Constituency Office:
Barking Learning Centre, 2 Town Square, Barking, IG11 7NB
margarethodge@hotmail.co.uk
07707045254 or 07595970515
www.margarethodgemp.com

Dame Margaret Hodge MP
Member of Parliament for Barking
House of Commons, London SW1A 0AA
Tel: 020 7219 6666

legal but harmful content, including a reporting system (for users to complain about content). Most providers – those in Category 2 – need only have reporting systems for illegal content. Category 1 services will also need to conduct and publish up-to-date assessments of their impact on freedom of expression and demonstrate they have taken steps to mitigate any adverse effects. Category 2 companies do not.

Clause 59 relates to the categorisation of social media companies. It says that the Secretary of State can categorise different companies as 'One' or 'Two' by considering: the likely impact of the number of users of a service; its functionalities; and the level of risk of harm to adults from content that is harmful to adults disseminated by means of the service.[58] Functionalities is later described as how it works. Using this model, the Government estimates that less than 3% of platforms will be in scope, of which the vast majority will be "Category 2" platforms. Those in this category will not have to respond to the issue of content that is lawful, but harmful to adults.[59]

However, size alone should not be the only determinant factor, and 'functionality' is not necessarily enough either.[60] The risk of platforms like 8Chan, Bitchute, Gab is proven, yet they would not be classified under Category One using these measures.[61] Three high-profile mass murders committed in recent years by white supremacists had at least one thing in common: the murderers were on the relatively fringe social media platforms that have become a haven for white nationalists (listed above).[62] For example, the alleged El Paso, Texas, shooter who killed 23 people in 2019 posted an anti-immigrant manifesto on 8Chan platform prior to the attack.[63] In it, he expressed support for the accused shooter in Christchurch, New Zealand, who killed 51 people in two mosques and also used 8Chan.[64]

If these platforms are not in Category 1, the Bill will not be fulfilling its purpose.

4.1 Recommendation

The categorisation of social media companies in the bill needs amending. The requirements imposed on Category One companies must be extended to those platforms known to ferment violent extremism. For example, those platforms on the risk register developed and

[58] Ibid.
[59] Antisemitism Policy Trust (December 2020), *'Government's Online Harms White Paper Response,'* https://antisemitism.org.uk/wp-content/uploads/2020/12/A-prelude-to-the-online-safety-bill-December-2020-FINAL-1.pdf, p. 4.
[60] Ibid.
[61] Luke Munn (2020), '*Angry by design: toxic communication and technical architectures*,' pp. 2-3.
[62] Ibid.
[63] Ibid.
[64] Jonathan A. Greenblatt (Dec 2020), 'Stepping Up to Stop Hate Online,' https://ssir.org/articles/entry/stepping_up_to_stop_hate_online#.

Dame Margaret Hodge MP
Member of Parliament for Barking
House of Commons, London SW1A 0AA
Tel: 020 7219 6666

maintained by OFCOM should be captured by these regulations, in order to ensure violent and extreme language on these platforms can be removed swiftly.[65] Furthermore, the provisions around 'legal and harmful' language must be extended to Category Two companies.

The European Union's proposal for a Digital Services Act can be used as a template to ensure more platforms are covered. Their bill gives clear definitions of online platforms and very large platforms (at least 45 million average monthly users in the union), to ensure most are encompassed by their regulations.[66]

Question Five: Are children effectively protected from harmful activity and content under the measures proposed in the draft Bill?

As stated in Question One, the OSB stemmed from concern for the harm children face online. However, children's campaigners have expressed two concerns to me regarding children's safety online, which will be addressed in turn. Firstly, the amendment to the Digital Economy Act, and secondly, the issue of end-to-end encrypted messages.

5.1 Digital Economy Act

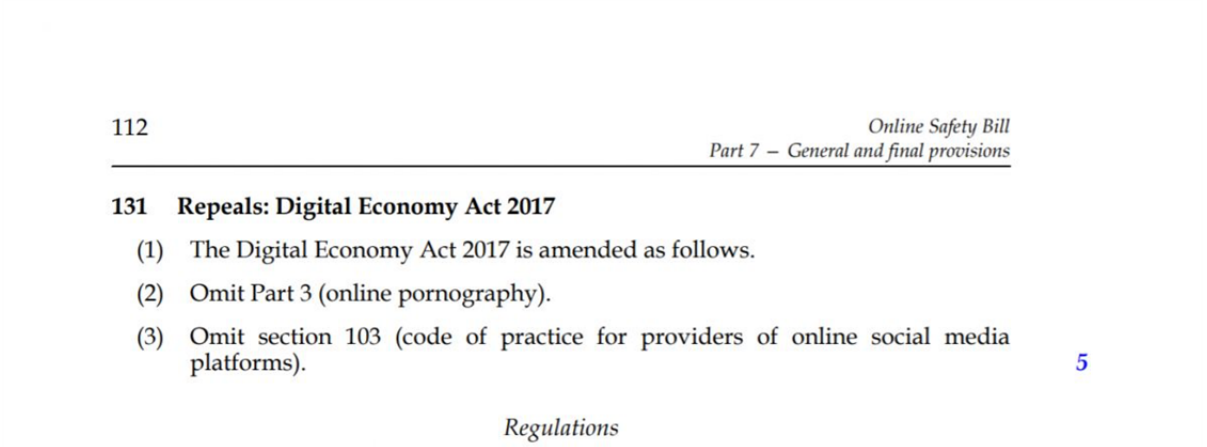
Children's campaigners are concerned that the bill fails to ensure sites that publish hardcore porn are adequately monitored by OFCOM. They have argued that the draft bill does not allow OFCOM to confirm that these sites are enforcing age-verification tools, as it overturns pre-existing regulation which ensured this and protected children.[67] This means children will be left in a more vulnerable position under this legislation than previously.

The concerns stem from the fact that the Government's OSB intends to repeal Part 3 of the Digital Economy Act (DEA).[68]

[65] Antisemitism Policy Trust (December 2020), *'Government's Online Harms White Paper Response,'* https://antisemitism.org.uk/wp-content/uploads/2020/12/A-prelude-to-the-online-safety-bill-December-2020-FINAL-1.pdf, p. 4.
[66] Edina Harbinja, '*U.K.'s Online Safety Bill: Not That Safe, After All?,'* https://www.lawfareblog.com/uks-online-safety-bill-not-safe-after-all
[67] Jonathan Chadwick (May 2021), '*Campaigners are 'astonished' by a loophole in the government's draft Online Safety Bill that could put pornography sites 'outside its scope'*,' Daily Mail, https://www.dailymail.co.uk/sciencetech/article-9592385/Expert-concerned-lack-porn-age-checks-Online-Safety-Bill.html
[68] See Figure One.

Constituency Office:
Barking Learning Centre, 2 Town Square, Barking, IG11 7NB
margarethodge@hotmail.co.uk
07707045254 or 07595970515
www.margarethodgemp.com

Dame Margaret Hodge MP
Member of Parliament for Barking
House of Commons, London SW1A 0AA
Tel: 020 7219 6666



112 *Online Safety Bill*
Part 7 – General and final provisions

131 Repeals: Digital Economy Act 2017

(1) The Digital Economy Act 2017 is amended as follows.

(2) Omit Part 3 (online pornography).

(3) Omit section 103 (code of practice for providers of online social media platforms).

Regulations

Figure 1: Draft Online Safety Bill, Section 131

Part 3 of the DEA includes robust age verification on all commercial pornographic websites by the BBFC.[69]

In comparison, the new Bill concentrates only on 'user-generated' pornographic content, primarily found on social media and on some websites. Meanwhile, popular porn websites, such as Pornhub, which have sponsored videos, will no longer be required to age verify content.[70] This means that any porn sites which have user-generated content may remove this to dodge regulation, with no impact on their revenues or business model.[71]

Secondly, the draft bill states that OFCOM will not be given the power to remove illegal, pornographic material (namely, child pornography) until 2023. This leaves children vulnerable. These powers must come into force as soon as the legislation is passed, in order to ensure illegal pornographic content is removed and reported straight away, and children are kept safe online.

5.1.1 Recommendation

OFCOM must be given significant powers and the resources to monitor all online pornography, not just user-generated content, and have the ability to remove illegal content where applicable.

[69] Digital Economy Act (2017), Part 3, https://www.legislation.gov.uk/ukpga/2017/30/contents/enacted
[70] CARE (May 2021), '*New Online Safety Bill – but what does it mean?,*' https://care.org.uk/news/2021/05/new-online-safety-bill-but-what-does-it-mean
[71] Digital Economy Act (2017), Part 3, https://www.legislation.gov.uk/ukpga/2017/30/contents/enacted

Constituency Office:
Barking Learning Centre, 2 Town Square, Barking, IG11 7NB
margarethodge@hotmail.co.uk
07707045254 or 07595970515
www.margarethodgemp.com

Dame Margaret Hodge MP
Member of Parliament for Barking
House of Commons, London SW1A 0AA
Tel: 020 7219 6666

5.2 End-to-end encrypted messages

Secondly, the Draft Bill does not mention the issue of end-to-end encrypted messages. Despite the OSB aiming to keep children safe online by finding and removing harmful content, harmful content sent on messaging platforms is currently not decryptable. This leaves children exposed to harmful messaging which cannot be traced. And yet the OSB is silent on this issue and does not grant OFCOM the power to decode these messages. Interventions from the NSPCC have warned that the ambiguity surrounding this issue will make preventing child sexual abuse more difficult.[72] Those who are involved in child sexual abuse are more commonly using messaging platforms such as Instagram, Facebook Messenger, Snapchat and WhatsApp, all of which use end-to-end encrypted codes. This means messages cannot be decrypted by social media companies or any regulators, and only the person receiving/ sending a message can access this content. The police have also expressed concern that this is problematic for tracking down and decoding terrorist content, or those spreading terrorist material.[73]

Without the mechanisms or legislation to allow these messages to be decrypted by OFCOM, the Government are allowing vulnerable children to have unfettered access to encrypted messaging, thus putting them at increased risk of sexual abuse.

5.2.1 Recommendation

There are numerous ways this could be resolved, including restricting the time children are allowed to spend on these apps, implementing key word lockouts using artificial intelligence, and biometric facial recognition. Apple have recently developed software that could flag illegal images, which are recorded on a central database, present on someone's smartphone before they enter end-to-end encrypted messages. This would allow the image and the sender to consequently be traced. What is clear, however, is OFCOM must be granted the power to be able to decrypt these messages, either through artificial intelligence or manually, in order to track down and prevent gangs from sexually abusing children.

[72] NSPCC, '*End-To-End Encryption: Understanding the impacts for child safety online*,' April 2021, https://www.nspcc.org.uk/globalassets/documents/news/e2ee-pac-report-end-to-end-encryption.pdf
[73] Mark Hookham, '*Counter-terrorism chief warns that Facebook's plan to encrypt billions of messages will stop the police foiling extremist plots and 'put lives at risk*,' Daily Mail, 31 January 2021, https://www.dailymail.co.uk/news/article-9206087/Counter-terror-chief-warns-Facebooks-plan-encrypt-messages-stop-police-foiling-plots.html

Constituency Office:
Barking Learning Centre, 2 Town Square, Barking, IG11 7NB
margarethodge@hotmail.co.uk
07707045254 or 07595970515
www.margarethodgemp.com

Dame Margaret Hodge MP
Member of Parliament for Barking
House of Commons, London SW1A 0AA
Tel: 020 7219 6666

Question Six: Are there any types of content omitted from the scope of the Bill that you consider significant e.g. commercial pornography or the promotion of financial scams? How should they be covered if so?

There are three key elements omitted from the draft OSB which should be included in order for the legislation to effectively deliver the policy aim of "making the UK the safest place to be online."[74] These are: anonymous abuse, liability for chief executives, and extending the regulations of fraud to paid advertisements. Each will be addressed in turn.

6.1 Anonymous abuse

There is no mention of anonymous abuse in the bill. However, anonymous abuse is severely contributing to online hate. In the first decade of social media, we hesitated to hold social media companies fully responsible for the rising levels of abuse, incivility, and misinformation on the platforms they built and profited from.[75] Individual victims were encouraged to be resilient, and to report and block their abusers. Everyone else was encouraged to "not feed the trolls". However, now there's overwhelming evidence that social media users who feel unidentifiable are more likely to engage in rude and abusive behaviour & spread misinformation.[76] Anonymous abuse is not just hateful in itself but is used to spread lies about individuals and aims to undermine their credibility and so shut down their voices.[77] Therefore, far from nurturing democratic debate, voices and opinions are silenced and undermined.

Furthermore, anonymous abuse has been ever more noticeable over the course of the pandemic, particularly against women and girls.[78] It is understandable why people turned to social media to stay in touch, prevent loneliness and keep entertained whilst we have had spells in lockdown. Amongst these positive aspects of social media, the Internet is being used by hateful individuals to send abuse – most often anonymously – to others, often to Members of Parliament.[79]

---

[74] Department for Digital, Culture, Media and Sport (2021), '*Draft Online Safety Bill*,' https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf.
[75] David Babbs (January 2020), '*New year, new internet? Why it's time to rethink anonymity on social media*,' Open Democracy, https://www.opendemocracy.net/en/opendemocracyuk/new-year-new-internet-why-its-time-rethink-anonymity-social-media/
[76] Ibid.
[77] Dame Margaret Hodge (March 2021), '*Hansard: Online Anonymity and Anonymous Abuse*,' https://hansard.parliament.uk/commons/2021-03-24/debates/378D3CBD-E4C6-4138-ABA6-2783D130B23C/OnlineAnonymityAndAnonymousAbuse
[78] End Violence Against Women and Girls (September 2020), 'Online abuse during Covid: Almost half of women have experienced abuse online during pandemic,' https://www.endviolenceagainstwomen.org.uk/online-abuse-during-covid-almost-half-of-women-have-experienced-online-abuse-during-pandemic/

Constituency Office:
Barking Learning Centre, 2 Town Square, Barking, IG11 7NB
margarethodge@hotmail.co.uk
07707045254 or 07595970515
www.margarethodgemp.com

Dame Margaret Hodge MP
Member of Parliament for Barking
House of Commons, London SW1A 0AA
Tel: 020 7219 6666

For example, Following the Euro 2020 final on Sunday 11 July, the three black England footballers who missed penalty kicks faced a flood of online racial abuse. The abuse mostly came from anonymous social media accounts, which prompted an inflammatory debate on ending anonymity online.[80] As it turns out, this is not a controversial issue. According to a YouGov survey, 78% of British people are in favour of requesting the users to disclose their real identity when signing up on social media.[81]

However, I am of the view that anonymity must remain in place. Domestic violence victims need to remain anonymous, and we know that many young people have found a safe community online through maintaining their anonymity, such as LGBTIQ+ children and young people, and whistle-blowers also need to remain behind an unidentified identity.

It is not anonymity that needs to be stamped out, but anonymous abuse. Different types of online activity require different levels of accountability and/or different attributes to be verified.[82] If people are aware when they create a social media account that they are traceable, which doesn't necessarily mean identifiable, their behaviours and actions would change. This we have seen with the introduction of licence plates on cars. People are anonymous, however the knowledge that they could be traced if they broke the highway code, through speeding or dangerous driving, alters their behaviour to keep road users safe. This analogy can be applied to the internet.

Furthermore, if the bill is wanting to differentiate between the standards imposed on child users in comparison to adult users, it is difficult to comprehend how not having a 'know your user' approach would allow this to go ahead. Either the stringent duties which are being imposed on services with child users must be universally applicable, or a system that allows a third-party to trace users (not removing anonymity but ensuring users who abuse the platform can be held accountable) must be developed.

Therefore, there should be a system where anonymity is allowed but social media companies would have the ability to trace their users, in order to hand over information in criminal or defamation cases (similar to PayPal).[83] It is traceability, not identification, that is needed. Regulation therefore shouldn't impose a "one size fits all" approach on all businesses. Instead, it should set minimum standards to ensure that platforms can't just wash their hands of the challenges of ensuring accountability or the risks associated with

---

[79] Ibid.
[80] Luca Bertuzzi (July 2021), '*Online racial abuses in the UK prompt calls to end anonymity online*,' https://www.euractiv.com/section/digital/news/online-racial-abuses-in-the-uk-prompt-calls-to-end-anonymity-online/
[81] Ibid.
[82] Digital Policy Alliance (June 2021), '*Age/Identity Verification – Challenges, Solutions and Benefits*.'
[83] PayPal, '*How do I confirm my identity? (CIP),*' https://www.paypal.com/us/smarthelp/article/FAQ734

Constituency Office:
Barking Learning Centre, 2 Town Square, Barking, IG11 7NB
margarethodge@hotmail.co.uk
07707045254 or 07595970515
www.margarethodgemp.com

Dame Margaret Hodge MP
Member of Parliament for Barking
House of Commons, London SW1A 0AA
Tel: 020 7219 6666

anonymous abuse. If a platform fails to take an effective "know your user" approach or ensure that its users can be held accountable for their behaviour or their content, then the platform should be held accountable instead.[84]

Furthermore, smaller start-ups should be encouraged and supported in implementing this standard of accountability, in contrast to the rhetoric from the Government that these regulations would 'deter business.' Successful UK businesses are already rising to the challenge of building a trusting, accountable social media environment. For example, the video sharing platform VuePay allows unverified users to access all-age content but operates a sliding scale of verification requirements for users wishing to share content, access age-restricted content, or interact with other users.[85] While the Online Harms Bill does not necessarily need to address age verification, it goes to show that the technology is there to ensure users are accountable.

Conversations with the Digital Policy Alliance have shown that much of the thinking regarding age verification, set down in BSI PAS1296,[86] is relevant to developing approaches to verification of other attributes which would allow users to remain anonymous while they are not spreading abuse. This model, briefly, can allow a site to confirm a person's identity through a third-party provider which already has this person's details (for example, a bank). This third party can then send an encrypted code to the platform to verify their user's details, but without giving away private information. This code can be decrypted and retrieved if a user abuses a platform. This standard is now supported by the DCMS and in the process of becoming an international ISO standard.[87]

Therefore, it is possible to implement a standardised system whereby social media companies 'know their user' and can trace someone who violates their terms and conditions. The principles which should be applied when implementing this are:

- Data minimisation - the amount of data collected/shared and the length of time it is retained, for verification purposes should be the absolute minimum.
- Third-party options - don't force people to verify through one mechanism, or via the platform itself. A platform that already holds your information (such as a bank) can verify to the social media platform your identity through an encrypted code, so your details cannot be abused.[88]

6.1.1 Recommendation

[84] Digital Policy Alliance (June 2021), '*Age/Identity Verification – Challenges, Solutions and Benefits*.'
[85] See www.VuePay.com and www.GoBubbleWrap.com.
[86] The technology used in BSI PAS1296 can be accessed at:
https://shop.bsigroup.com/ProductDetail?pid=000000000030328409
[87] Digital Policy Alliance (June 2021), '*Age/Identity Verification – Challenges, Solutions and Benefits*.'
[88] Ibid.

Dame Margaret Hodge MP
Member of Parliament for Barking
House of Commons, London SW1A 0AA
Tel: 020 7219 6666

In summary, we need to make sure people are held accountable for what they do online, and we need to make sure that the absolutely shocking stories we have heard about anonymous abuse cannot be repeated. This is also a cross party issue – Conservative MPs such as Siobhan Baillie MP have been calling for this.[89] The amount of misogynistic abuse levelled at female MPs means, no matter their party, there is consensus on this issue. We can work together on this. Using the model outlined by the Digital Policy Alliance, users of social media companies would be able to remain anonymous, until they violated the platform's terms and conditions, allowing anonymous abuse to be prevented.

Furthermore, regarding the legitimate concerns organisations such as Stonewall have with anonymity online, any development in this area must be done in conjunction and consultation with minority groups who are unfairly affected by this issue. For example, an 'equality duty' on verification processes may help to ensure those with legitimate reasons for remaining anonymous can stay so.

6.2 Criminal liability for CEOs

The second omission from the OSB is holding Chief Executives of social media companies personally liable. Instead, a new criminal offence for senior managers has been included as a deferred power.[90] This could be introduced at a later date if tech firms do not step up their efforts to improve safety. In its place, currently, the main source of deterrence is set out as fines of up to 10% of a platform's revenue. This will be enforced by OFCOM if a company does not uphold its Terms and Conditions.[91]

However, I believe immediate and further sanctions on the individuals and directors of the platforms would be more effective in providing a deterrent incentive to ensuring the companies behave appropriately. A fine on a company will be seen as a cost on business. A fine on the director is a much more powerful way of ensuring responsible behaviour by companies.

Therefore, the bill must include personal liability for the directors of the social media companies.[92] The delay to the introduction of the power to hold directors liable until at

[89] Siobhan Baillie MP (March 2021), 'Hansard: Online Anonymity and Anonymous Abuse,' https://hansard.parliament.uk/commons/2021-03-24/debates/378D3CBD-E4C6-4138-ABA6-2783D130B23C/OnlineAnonymityAndAnonymousAbuse
[90] Department for Digital, Culture, Media and Sport (2021), '*Draft Online Safety Bill*,' https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf.
[91] Ibid.
[92] Jessica Elgot (December 2020), *'Margaret Hodge calls for ban on social media anonymity,'* The Guardian, https://www.theguardian.com/society/2020/dec/06/margaret-hodge-calls-for-ban-on-social-media-anonymity

Dame Margaret Hodge MP
Member of Parliament for Barking
House of Commons, London SW1A 0AA
Tel: 020 7219 6666

least two years after the regulation comes into force, following a review of the regulatory framework, does not represent the swift, sharp, regulatory action needed.[93]

As I explored in Chapter Two, social media's algorithms are directing people towards extreme opinions and conspiracy theories because it's a better way of holding an audience. The directors must bear some liability for the consequences of that activity. A Wall Street Journal report revealed in 2018 that Facebook executives were aware its recommendation engine stoked divisiveness and polarisation with negative consequences to society.[94] The report said Facebook's leadership ignored the findings and tried to absolve the company of responsibility for this polarisation, because the changes might disproportionately affect conservative users and hurt engagement.[95]

6.2.1 Recommendation

With other industries, we've created rules and regulations to protect public health. We should create a liability for the social-media companies so that they act against networks and known organisations that are putting out information that could lead to real-world harm (as discussed in Question Four).

6.3 Fraud via advertising

The final omission within the draft bill is its failure to extend its scope to fraud via advertising, emails or cloned websites (financial harms). In essence, paid-for fraud through adverts will not be in scope because the Bill focuses on harm committed through user-generated content. Although the Government has pledged to publish a Fraud Action Plan after the 2021 Spending Review and the Department for Digital, Culture, Media and Sport (DCMS) has said it will consult on online advertising, including the role it can play in enabling online fraud, later this year, the OSB is the perfect opportunity to tackle this pressing issue now.[96]

This is a pressing issue devastating so many lives currently. According to Action Fraud figures, in the UK alone, £1.7 billion was lost to scams in the past year, while estimates for the year to June 2020 reveal that 85% of all fraud was cyber-enabled.[97] Reports skyrocketed

[93] 5Rights Foundation (2021) '*Ambitions for the Online Safety Bill.'*
[94] Jeff Horwitz and Deepa Seetharaman, '*Facebook Executives Shut Down Efforts to Make the Site Less Divisive*,' The Wall Street Journal, https://www.wsj.com/articles/facebook-knows-it-encourages-division-top-executives-nixed-solutions-11590507499?mod=hp_lead_pos5
[95] Ibid.
[96] Department for Digital, Culture, Media and Sport (December 2020*), 'Online Harms White Paper: Full government response to the consultation,'* https://www.gov.uk/government/consultations/online-harms-white-paper/outcome/online-harms-white-paper-full-government-response.

Constituency Office:
Barking Learning Centre, 2 Town Square, Barking, IG11 7NB
margarethodge@hotmail.co.uk
07707045254 or 07595970515
www.margarethodgemp.com

Dame Margaret Hodge MP
Member of Parliament for Barking
House of Commons, London SW1A 0AA
Tel: 020 7219 6666

with the pandemic, and nearly one in four reports of scams reported mentioned a social media hook – 94% being on Instagram or Facebook. The Money and Mental Health Policy Institute found, nationally, 31% of people with recent experience of a mental health problem have felt stressed and 22% have felt depressed as a result of online scams.[98]

Consumer regulators such as the Financial Conduct Authority (FCA) and charities including the Money and Mental Health Policy Institute are urging the Government to reconsider and include these fraudulent scams in the bill.[99] Not doing so leaves a large proportion of the public at high risk of being scammed online, because criminals are experts in adapting their tactics to exploit any loopholes.

Currently, social media companies are benefitting financially from the laws around scam ads. They are paid by these fraudulent companies for running their adverts, but they are also paid by the FCA to have legitimate websites placed above scam ads in search engines. Therefore, it is a 'win win' for them, and morally unacceptable.[100] The FCA invested £600,000 into preventing scam adverts just on Google in 2020, generating a significant profit, yet this investment had little impact.[101] The question remains why the bill is therefore not addressing fraudulent, paid-for advertisements.

This immoral revenue will now only increase under the OSB. With the bill focusing on clamping down on user generated content, there is an incentive for fraudulent companies to instead pay to run their ads, instead of having users promote their content, so they escape the regulations. This will continue to benefit the fraudsters and chief executives.[102]

Furthermore, at the moment, the framework in place on social media sites removes false ads once they have been identified and someone has been a victim and lost money. This is problematic: in 2020 £570 million was lost to scam ads, and only £200 million of that was returned to customers due to the lack of infrastructure to find non-existent companies.[103]

---

[97] Action Fraud (May 2021), '*New figures reveal victims lost over £63m to investment fraud scams on social media*,' https://www.actionfraud.police.uk/news/new-figures-reveal-victims-lost-over-63m-to-investment-fraud-scams-on-social-media
[98] Money and Mental Health Policy Institute (2021), '*Put scams in the Online Safety Bill, or leave millions of vulnerable people at risk of financial harm", warns Martin Lewis charity*,' https://www.moneyandmentalhealth.org/press-release/press-release-safety-net-online-safety-bill/
[99] Ibid.
[100] Money Saving Expert (July 2021), '*Online Safety Bill 'doomed to fail' unless it includes scam adverts, Martin Lewis and campaigners warn,*' https://www.moneysavingexpert.com/news/2021/07/government-s-online-safety-bill-doomed-to-fail/
[101] Financial Conduct Authority (May 2021), 'The rise in scams and the threat to a legitimate financial services industry,' https://www.fca.org.uk/news/speeches/rise-scams-and-threat-legitimate-financial-services-industry
[102] Money Saving Expert (July 2021), '*Online Safety Bill 'doomed to fail' unless it includes scam adverts, Martin Lewis and campaigners warn.'*
[103] Ibid.

Dame Margaret Hodge MP
Member of Parliament for Barking
House of Commons, London SW1A 0AA
Tel: 020 7219 6666

There are very limited checks on these sites beforehand to ensure the advertisement is not fraudulent. For example, in under an hour, the adverts Which? created for both fake businesses were approved by Google; they garnered nearly 100,000 impressions over the space of a month.[104] Google just requires advertisers to have a Gmail account to create adverts and while it did review adverts submitted, it did not verify if the business existed or was legitimate, nor ask for proof of ID.[105]

There should be a system in place where Corporations have to vet the advertisements they are making a profit on before they appear on their platform, to ensure they are legitimate. If not, they should face penalties.

6.3.1 Recommendation

- The bill should extend the provisions already within the bill regulating user-generated content to paid-for advertisements to clamp down on fraudulent ads on social media platforms.
- The bill should mandate an 'ex-ante' system on all social media platforms, ensuring they check all advertisements before they appear on their platform, as opposed to an 'ex-poste' system, to ensure more fraudulent ads are caught before a victim is scammed.

Question Seven: The draft Bill specifically places a duty on providers to protect democratic content, and content of journalistic importance. What is your view of these measures and their likely effectiveness?

This is a wider concern with the scope of the bill, carrying on from Question Four. The Bill's scope is subject to widely drawn exemptions for services deemed to pose a low risk of harm to users, or that are otherwise regulated. Crucially, content on news publishers' websites is also excluded from the scope of the legislation. Clause 18 of the bill outlines that the duty of care outlined in Chapter 2 (duty of care is defined as methods to 'minimise' the presence, length of time, availability of illegal content) does not extend to the content present on the website of a recognised news publisher.[106]

Content of democratic importance has already been covered in Question Two, however, the exception for content of journalistic importance is also deeply problematic. Self-regulation

[104] Ibid.
[105] Ibid.
[106] Department for Digital, Culture, Media and Sport (2021), '*Draft Online Safety Bill*,' https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf

Constituency Office:
Barking Learning Centre, 2 Town Square, Barking, IG11 7NB
margarethodge@hotmail.co.uk
07707045254 or 07595970515
www.margarethodgemp.com

Dame Margaret Hodge MP
Member of Parliament for Barking
House of Commons, London SW1A 0AA
Tel: 020 7219 6666

has failed which is why this Bill exists. Allowing such websites with comments boards to have no duty of care is illogical.

What classifies as journalistic importance is far too broadly defined. One perverse consequence is that one of the legal definitions of what a 'recognised news publisher' sets a low bar for what is considered journalism online, by being too broad and not demanding real accountability and proven adherence to any recognised standards code. This therefore opens the door to large amounts of content that in practice will remain completely unregulated, although they will still be greenlit as 'news content'.[107]

Furthermore, if the criteria for what amounts to journalism is too wide, publishers will be free to publish harmful content (broadly, where there is a material risk of adverse psychological or physical impact on children, or people with certain characteristics),[108] without any regulatory oversight.[109] The proposed legislation does not address this risk. Rather, it entrenches it.

For example, some of the highest profile and dangerous far-right figures in the UK, including Stephen Yaxley-Lennon (also known as Tommy Robinson) now class themselves as journalists. Would this protection mean that his content would receive additional protections? There are also far right and conspiracy theory "news companies" such as Rebel Media and Alex Jones' InfoWars. These both replicate mainstream news publishers but are used to spread misinformation and discriminatory content. Would they receive additional protections under this clause of the bill? Under this proposed draft, it could be the case that racist and misogynist content that is legal could be re-uploaded and unregulated if the content in question was uploaded on to one of these websites or produced by a journalist.[110]

Comment boards on journalistic websites are also exempted from regulations in the OSB (section 14).[111] This allows people to still spread hateful material online in this format.

<u>7.1 Recommendation</u>

[107] Lexie Kirkconnell-Kawana (June 2021) '*Online Safety Bill: Five thoughts on its impact on journalism*,' LSE Blogs, https://blogs.lse.ac.uk/medialse/2021/06/03/online-safety-bill-five-thoughts-on-its-impact-on-journalism/
[108] See pages 39-40 on the OSB for more detail on this.
[109] Lexie Kirkconnell-Kawana (June 2021) '*Online Safety Bill: Five thoughts on its impact on journalism*.'
[110] HOPE Not Hate, 'Our Response To The Draft Online Safety Bill,' https://www.hopenothate.org.uk/2021/06/07/hope-not-hates-response-to-the-draft-online-safety-bill/
[111] Department for Digital, Culture, Media and Sport (2021), '*Draft Online Safety Bill*,' https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf

Dame Margaret Hodge MP
Member of Parliament for Barking
House of Commons, London SW1A 0AA
Tel: 020 7219 6666

The Government must amend this clause to ensure harmful content published by journalists can be removed, and existing regulators/regulated publications have measures in place to address harm on relevant comment boards.

Question Eight: Are Ofcom's powers under the Bill proportionate, whilst remaining sufficient to allow it to carry out its regulatory role? Does Ofcom have sufficient resources to support these powers?

The OSB proposes that OFCOM will be appointed as the online harm's regulator.[112] This means it will be responsible for helping companies to comply with the new laws by publishing codes of practice, and it will oversee the way that companies tackle illegal content on their services and protect children from harmful and inappropriate content. However, there are four concerns I have with this, which will each be addressed in turn.

8.1 Self-regulation

The proposals for OFCOM's monitoring still in essence require self-regulation by the platforms themselves, which is not working. As explored in Question Two, all social media companies that fall under this regulatory framework will need to be able to show that they are meeting their duty of care through their Terms and Conditions, and the regulator will use this to decide how well online harm is being addressed by assessing if these terms and conditions are kept to 'consistently' and how online hate is 'dealt with,' rather than using their independent understanding of preventing harm.[113] This will not ensure online hate is tackled swiftly.

8.2 Fines

While Ofcom will be given the power to fine companies up to £18 million, or ten per cent of qualifying revenue, if they fail in their new duty of care, it is unclear in the draft bill how this will be enforced.[114] The Government needs to develop this more, as this is currently their main source of deterrence if personal liability is not being introduced. Similarly, while companies generating revenue above a threshold (based on global annual revenue) will have to notify Ofcom and pay an annual fee, the threshold is likely to be high enough to mean this will only apply to a small number of businesses. Therefore, again, this will just become another 'cost of doing business,' and is not a deterrent.

[112] Ibid.
[113] Ibid.
[114] Ibid.

Constituency Office:
Barking Learning Centre, 2 Town Square, Barking, IG11 7NB
margarethodge@hotmail.co.uk
07707045254 or 07595970515
www.margarethodgemp.com

Dame Margaret Hodge MP
Member of Parliament for Barking
House of Commons, London SW1A 0AA
Tel: 020 7219 6666

8.3 Reporting

Thirdly, when it comes to reporting, companies of both categories (1 and 2) will be required to follow Ofcom's guidance around "producing an annual transparency report" which will be subject to Ofcom's requirements.[115] However, this is an ex-poste approach, as opposed to ex-ante. In short, Ofcom will not be made aware of failures by companies to remove online harm until a year after it has happened; a year after the abuse harmed an individual. For future rules to work, Ofcom will need strong powers to obtain real-time information from internet companies, and demand it is taken down immediately.

8.4 Capacity

Finally, there are concerns around OFCOM's regulatory capacities and suitability.[116] For example, OFCOM will be required to set up an advisory committee on disinformation and misinformation ("fake news"), comprised of "persons with expertise in the prevention and handling of disinformation and misinformation online." Therefore, the bill creates a powerful online regulator, with potent enforcement mechanisms, which could have significant and lasting effects on businesses and digital rights. However, there is a real danger that OFCOM may not be able to undertake this role effectively, given all the other areas within its regulatory remit, plus its lack of human and technical capacity.[117]

8.5 Recommendations

Four in five adult internet users have concerns about going online, and most people support tighter rules – we need more powers and regulations given to this body to ensure OFCOM have the ability and resources to uphold the duty of care.[118]

- OFCOM must develop its own understanding of what constitutes 'harmful content' and how companies can implement this within their terms and conditions, in order to hold all platforms to a high standard.
- How the fines given to platforms in breach of their terms and conditions need to be more clearly defined in the bill to ensure it can be implemented by OFCOM.
- The present government proposal for only an annual transparency report from tech companies is one of the inadequate proposals that must be addressed: retrospective

[115] Ibid.
[116] Edina Harbinja, '*U.K.'s Online Safety Bill: Not That Safe, After All?'*
[117] Ibid.
[118] OFCOM (February 2020), '*Internet users' experience of potential online harms: summary of survey research*,' https://www.ofcom.org.uk/__data/assets/pdf_file/0024/196413/concerns-and-experiences-online-harms-2020-chart-pack.pdf

Dame Margaret Hodge MP
Member of Parliament for Barking
House of Commons, London SW1A 0AA
Tel: 020 7219 6666

reports don't provide timely information when it's needed by stakeholders to address online harms.

- Furthermore, the regulator must be given power and resources to demand material is taken down from the internet as soon as they are aware, as is the case in Australia.[119]
- OFCOM needs to be equipped with more resources in order to function efficiently and effectively with its new remit.

9. Conclusion

I hope these considerations are helpful in the next stage of your inquiry and am grateful for being provided with the opportunity to respond.

Dame Margaret Hodge MP
Chair, APPG on Anti-Corruption and Responsible Tax

6 October 2021

[119] Chris Duckett (2019), '*New Australian Online Safety Act to include take-down of cyber abuse*,' https://www.zdnet.com/article/new-australian-online-safety-act-to-include-take-down-of-cyber-abuse/

Constituency Office:
Barking Learning Centre, 2 Town Square, Barking, IG11 7NB
margarethodge@hotmail.co.uk
07707045254 or 07595970515
www.margarethodgemp.com