

Dr Edina Harbinja¹

Online Safety Bill (Lords Communications and Digital Committee)

I am grateful for the opportunity to submit this letter to the Committee and expand on some of the issues raised at the Committee session on Tuesday, 6 December 2022.

In this submission, I would like to focus on the key clauses that require further scrutiny and amendments. I will focus on my concerns regarding the effects of clauses 15 – 17, 20 and 166 of the Bill (as amended on report). In a separate joint letter, I will detail my concerns related to clause 106 (Notices to deal with terrorism content or CSEA content (or both)).

1. Clauses 15 – 17: the distinction between content of democratic importance, news publisher content and journalistic content

As noted in my previous written and oral evidence to the Joint Committee and the DCMS Committee, the distinction between democratic and journalist content is vague and unnecessary, as set out in clauses 15 and 17 of the Bill. This has been exacerbated by the inclusion of clause 16 and the news publisher content. The three clauses aim to protect equally essential aspects of speech but offer very different protection mechanisms and remedies (e.g. ‘a dedicated and expedited complaints procedure’ for journalistic content in clause 17 or a detailed explanation of steps to be taken regarding the news publisher content in clause 16).²

Further, the content of democratic importance seems to include only political speech, which is much more restricted than categories of speech protected by Article 10 ECHR.

The Joint Committee on Human Rights echoes my concern, noting that it is unclear ‘what content falls within the heightened protections provided in relation to “content of democratic importance” and “journalistic content”’.³

Therefore, I propose that these three clauses be merged to provide the same level of protection for the most significant types of speech.

2. Clause 166 – Providers’ judgements about the status of content

The clause includes the illegality threshold of “reasonable grounds to infer”. The providers in scope will need to use this threshold to judge whether the content is illegal or represents fraudulent advertisement. Clause 167 provides that Ofcom will issue guidance concerning this judgement. This is problematic for many reasons. Notably, the threshold is very low and can mean that, in practice, providers will apply an overly cautious approach and remove content

¹ Reader in media/privacy law, Aston Law School, Aston University, <https://research.aston.ac.uk/en/persons/edina-harbinja>. The evidence provided reflects the views of the author.

² I have written about this in more detail here: Edina Harbinja and Mark R. Leiser, “[Redacted]: This Article Categorised [Harmful] by the Government” (2022) 19:1 SCRIPTed 88 <https://script-ed.org/?p=4050>
DOI: 10.2966/scrip.190122.88

³ Joint Committee on Human Rights, Letter to the Secretary of State for Digital, Culture, Media and Sport, 19 May 2022, <https://committees.parliament.uk/publications/22323/documents/165077/default/>

that may not be illegal and could consist of protected speech under the European Convention of Human Rights.

The threshold in clause 166 should be raised from “reasonable grounds to infer” to a more robust, established and precise threshold of “manifest illegality”.⁴

3. Clause 20 - Duties about freedom of expression and privacy

I would like to submit specific amendment proposals which will clarify and strengthen this clause. The clause, as drafted, conflates concepts of privacy and data protection and does not signal a clear intent to protect freedom of expression, privacy and users’ personal data.

Clause 20, page 21, line 42, leave out “have regard to the importance of protecting” and insert “protect”

Explanation:

The phrasing in the Bill is vague and does not offer strong assurances that users’ freedom of expression will be protected. The proposed change signals a more explicit obligation and provides a more succinct phrasing.⁵

Clause 20, page 21, line 43 leave out “within the law”.

Explanation:

The words are superfluous. Freedom of expression cannot be protected “outside the law”.

Clause 20, page 22, line 3 leave out “have regard to the importance of protecting users from a breach of any statutory provision or rule of law concerning privacy that is relevant to the use or operation of a user-to-user service (including, but not limited to, any such provision or rule concerning the processing of personal data).” and insert “their privacy and data protection rights”.

Explanation:

The formulation is unnecessarily complicated. It conflates the concepts of privacy and data protection. These are very different concepts that imply different obligations (e.g. privacy assumes respecting the user’s human rights, whereas data protection offers clear principles and mechanisms for the protection of personal data). As mentioned above, the proposed change also signals a more explicit obligation and provides a more succinct phrasing.

⁴ Poland v European Parliament and Council, (Case C-401/19, 26 April 2022), a decision of the CJEU applying ECHR caselaw to platform filtering obligations in the context of copyright., see also Graham Smith, ONLINE SAFETY BILL – SUBMISSION TO PUBLIC BILL COMMITTEE 26 May 2022, <https://bills.parliament.uk/publications/46665/documents/1879>

⁵ I have written about this in more detail here: Edina Harbinja and Mark R. Leiser, “[Redacted]: This Article Categorised [Harmful] by the Government” (2022) 19:1 SCRIPTed 88 <https://script-ed.org/?p=4050>
DOI: 10.2966/scrip.190122.88

Clause 20, page 22, line 15 leave out “within the law”

Clause 20, page 22, line 28 leave out “within the law”

Explanation:

This is consequential to the above proposal.

If this is accepted, there would be consequential amendments to clause 30 and elsewhere in the Bill where these formulations exist.

4. Coroner’s access to deceased children’s data

In the Committee session on 6 December 2022, there was a brief mention of the proposal to allow the coroner’s and/or the bereaved parent access to children’s personal data and communications. I support mandating the coroner’s access. However, I cannot support a default family access to children’s social media accounts, personal data and communications. I have written extensively about the notion of post-mortem privacy, and this applies to the protection of children’s privacy as well⁶ Additionally, the default access by parents would enable them to access personal data and communication of third persons, social media friends and other users with whom the child has communicated and violate their expectations of privacy.

I am happy to discuss all this further with the Committee during the Lord’s scrutiny sessions.

Sincerely,

Dr Edina Harbinja

12 December 2022

⁶ See, for example, Edina Harbinja, *Digital Death, Digital Assets and Post-mortem Privacy*, (Edinburgh University Press, 2022),