Online Safety Call for Evidence
Ofcom
Riverside House
2A Southwark Bridge Road
London, SE1 9HA

September 2022

Dear Sir/Madam,

Please accept this letter as my submission to the call for evidence for the first phase of online safety. My role as Member of Parliament means that my focus is primarily concerning how we might strengthen legislation in order to provide the necessary framework for Ofcom to operate effectively as regulator. The intention is to provide for victims by creating useful law, while developing systems that can mitigate legal shortfalls in the meantime. I have chosen to answer four questions to this effect; Q2, Q7, Q27, and Q28.

Q2. Can you provide any evidence relating to the presence or quantity of illegal content on user-to-user and search services?

Many and varied groups suffer from harm caused by illegal online content, but women and girls in particular remain the targets of much of the intimidation and abuse that can be found on user-to-user and search services – a 27-times greater likelihood than men. According to a poll conducted by Ipsos MORI for Amnesty International in June 2017, 1 in 5 women in the UK have suffered online abuse or harassment, increasing to 1 in 3 for young women, and of those women suffering this abuse almost half reported it was sexist or misogynistic in nature. 27% were threatened with physical and sexual assault, and for female journalists, 20% said they have actually been attacked or abused offline in connection with the online abuse.

Victims of intimate image abuse are primarily female and the perpetrators are primarily male. Not only is the sharing of such images an offence in itself, but the offence is also linked to very real-world harms: the ONS report that conviction data for image based sexual abuse show that out of the 376 prosecutions for intimate-image abuse offences recorded in the year ending March 2019, 83% (313) were flagged as being domestic abuse-related. Such data only goes to accentuate that online harms are in no way confined to computer screens.

For these reasons, when compiling codes of practice and risk assessments, Ofcom must take a thematic consideration of women and girls, rather than considering them their own topic. Women and girls are the targets of offences across the spectrum, and they must not be thought of in isolation. Instead, codes of practice should, in each section, look at the likely impact on women and girls, and instate particular mitigations against the risks they disproportionately face.

Q7. What can providers of online services do to enhance the transparency, accessibility, ease of use and users' awareness of their reporting and complaints mechanisms?

Anecdotally, users have low levels of trust in flagging or reporting content to social media companies, and survey evidence is showing a decline in trust in social media more generally. Insider Intelligence recently reported that only 35% of US social media users felt safe participating and posting on platforms, making safety online ‘the second most significant factor affecting trust’, after privacy. The Edelman Trust Barometer 2022 reveals that ‘none of the major information sources are trusted as a source of news and information’ but social media is the least trusted source at only 37%. This is unsurprising given the increasing amounts of disinformation available on social media, leading Edelman to find that 76% of people are concerned that false information is being actively used as a weapon.

These statistics exposing the general lack of trust in social media platforms reflect the anecdotal distrust in reporting mechanisms. Data on the latter is difficult to come by, as platforms’ statistics on their post removal numbers rely on only those posts which are flagged to them, and do not reveal instances in which someone considers reporting material to be futile. However, a 2017 Ipsos MORI poll revealed that only 23% of Facebook and 19% of Twitter users in the survey rated the platforms’ response in addressing online abuse or harassment as adequate, versus 41% and 43% who considered it inadequate. The Center for Countering Digital Hatred looked specifically at the removal rate of flagged anti-Semitic social media posts which the Center considered to have ‘clearly violated’ community guidelines. The CCDH reported that only 84% of these flagged posts were not acted upon. If these statistics bear out for other categories of harmful or illegal content, it is understandable that users would consider this perceived inaction as uncaring, resulting in a loss of trust.

It seems reasonable to assume that, even with advancements in AI monitoring systems, the sheer volume of content on social media platforms is an obstacle to platforms handling complaints and flags in a way that users consider satisfactory. The perception that reports are evaluated by bots and not humans – whether or not this is accurate – does not help to develop trust in reporting. Accordingly, there must be a useable complaints system with the capacity to handle individual cases, and this system must be third-party. Ofcom’s regulatory role must be protected, and without a third-party body that can handle complaints regarding social media companies, it seems inevitable that Ofcom could become inundated with complaints that it hasn’t the capacity to handle appropriately and which could seriously damage its reputation. Equally, this function cannot be left in the hands of the platforms themselves given the already limited trust in the complaints procedure, and the risks posed by reduced objectivity of in-house complaint handling. An independent reporting mechanism available in situ on social media platforms, however, would work to bridge the gap, ensuring that reporting can be both convenient (links being readily available on a social media site itself) and independent of the platform (by redirecting to the third-party mechanism).

Users must feel that their concerns are being recognised and their complaints handled in an individualistic manner. While automation is effective for many purposes, it does not serve to create the sense that an issue has been heard and judged on merit in its context. In addition, the Treasury should create a pathway for fines levied by Ofcom to be distributed amongst victim support organisations so that trauma occurring in the aftermath of online abuse may be more effectively dealt with for those who need it.

Ofcom should encourage the establishment of a third-party reporting mechanism and complaint-handling body to ensure Ofcom can retain its role as regulator and allow complaints to be dealt with in an effective manner without taking from the extensive role Ofcom already performs.

Q27. For purposes of transparency, what type of information is useful/not useful? Why?

The importance of parliamentary scrutiny cannot be overstated when considering transparency and supporting the operation of Ofcom as it goes about producing transparency reports. Parliament and Ofcom must work in parallel with each focusing on different, but interrelated, metrics which will together inform future best practice. For example, while Part 4, Chapter 3, of the Bill stipulates the publishing of transparency reports by platforms and Ofcom, the power to close loopholes and rectify statutory issues revealed through these reports remains with Parliament. No amount of reporting will solve issues that have their root in the legislation, and accordingly Ofcom should support the creation of a parliamentary standing committee on online safety. It would be the role of this committee to stay abreast of reporting required under the Bill in order to identify the need for further legislative change that may become apparent as time goes on. One of the key reasons for bringing in an Online Safety Bill specifically is that our current legal framework, treating as it does online crimes largely as though they were crimes in the physical world, is no longer fit for purpose in the modern digital age. We risk placing ourselves in a similar situation sooner than we might expect, given the rapid advances in technology, if there is not a parliamentary body to note where and how updates in legislation are needed.

Such a standing committee would be able to take note of reports from platforms, while being mindful of Ofcom recommendations. It follows, therefore, that Parliament ought be considered as one of the intended audiences for transparency reports; a potential use-case would be a standing committee considering reports to highlight potential shortfalls in the existing statutory framework.

Information that would be useful to a parliamentary committee would centre around any previously unidentified harms that do not fall under the scope of legislation. Quantitative information would be useful as supporting data alongside qualitative analysis which would function to make clear where the committee should recommend measures to the relevant department.

Q28. Other than those in this document, are you aware of other measures available for mitigating risk and harm from illegal content?

As outlined in the response to Q27, continued parliamentary scrutiny will remain vital for identifying when and how existing law falls short in the light of new harms. That said, legislation is deficient in a number of aspects, even when taking into account the changes that will be enacted by the Online Safety Bill.

Directly updating the statutory framework is not in Ofcom’s power, yet it is undoubtedly one of the most effective measures that can be taken to further mitigate risk. It will remain the responsibility of Parliament to keep measures up to date in order that Ofcom can regulate most effectively. It is for this reason that continued engagement of Ofcom with Parliament will become more important once this Bill enters law, as we are dealing with a quickly moving legislative field.

The most pertinent example of an online harm which, under too-limited circumstances, is classed as illegal content is intimate image abuse. The law governing offences of sharing intimate images without consent is insufficient to deal with the scale and impact of the problem, as the Law Commission has identified. Should Parliament succeed in updating legislation to include all Law Commission recommendations on this topic, Ofcom will have better scope than it currently does to regulate how online platforms deal with images shared. From 2015–20 the Revenge Porn Helpline supported over 8,000 people and successfully removed nearly 200,000 pieces of content shared illegally, even though in recent years the rate of arrest following these offences was only 11%. This is, however, a growing issue that overwhelmingly affects women; caseload at the Revenge Porn Helpline increased by over 40% between 2020 and 2021, and on average a female victim contends with 42 images reported compared to two for male victims. There is, as yet, no clear timetable to rectify the legal omissions that fail to provide women with better protection, and an urgent pathway needs to be established for changes in law which will allow Ofcom to properly regulate platforms which host such harmful images. According to the Law Commission's report on intimate image abuse, 'the rapid developments in technology have also created new ways of offending. The use of deepfake pornography and nudification software is increasingly common,' meaning that new law will need to be constantly in the pipeline to keep up with these 'new ways of offending'.

Establishing an efficient legislative pathway that starts with identifying issues, to parliamentary consideration, leading to government action will be a key measure to mitigate risk and allow Ofcom to regulate accordingly.

Ofcom must show support for continued legislative review in this sphere so that firstly, that this review takes place and secondly, that it appropriately identifies legal deficiencies so that we may better serve victims of online crime.

Concluding Recommendations

As set out above, Ofcom should consider acting on the following:

1. A thematic consideration of women and girls when identifying harms in codes of practice and risk assessments, rather than an isolated 'women and girls' chapter.
2. Working to establish a third-party complaints mechanism with capacity to deal with individual cases.
3. Support for establishing a parliamentary Standing Committee on Online Safety to which Ofcom could submit transparency reports and recommendations for consideration of future necessary legislative changes.
4. Support for continued legislative review in order that the law can remain effective in the online safety domain.