Online Safety Bill – Public Bill Committee

Evidence Submission Professor Clare McGlynn, Durham University

Executive Summary

1. Regulating online abuse enhances freedom of speech of women & girls

2. Illegal content definitions and over-reliance on criminal law

Amend definition of illegal content to be flexible, leading to more effective regulation

- Service providers only obliged to act where content 'amounts to' a criminal offence, suggesting a high level of exactitude, with risk of less effective and comprehensive regulation.
- Recommend amending cl 52(2) to where service providers have 'reasonable grounds to believe' an offence has been committed, as in an earlier draft of the bill, or refer to "content of a kind', a term used in cl 53(4)(c) and cl 54(3)(b).

Amend Schedule 7 Priority Offences to include Scotland and Northern Ireland

- Schedule 7 does not include equivalent offences under Scots and Northern Irish law.

3. Limits and gaps in priority offences in Schedule 7

Limitations of extreme pornography offences

- Varying standards across the UK with Scots law most comprehensive
- Lack of clarity defining extreme porn including what constitutes 'obscene' materials
- Extreme porn does not include incest material

Limitations of non-consensual distribution of sexual images offence

- Amend English law to criminalise distribution of deepfake/altered images, following Scots law

4. Extend Schedule 7 to include more violence against women offences

- Modern Slavery Act 2015 – to include trafficking offences
- Cyberflashing
- Blackmail – to include offences relating to sexual extortion (sextortion/webcam blackmail)
- Obscene Publications Act 1959 – to include distribution of incest material

5. Extend Schedule 6 to include all child sexual offences

- Include child sexual offences involving abuse of position of trust

6. Revise cyberflashing offence so comprehensive, straightforward and consent-based

- cl 156 only covers *some* cases of cyberflashing on proof of specific motives to cause distress or sexual gratification and reckless regarding distress
- Considerable gaps in the law where images distributed for transactional reasons (to gain nudes in return) and to show off/gain kudos/male bonding
- Even where distress may be motive, requirement to evidence this motive will limit prosecutions
- Evidence from similar requirement in non-consensual distribution of sexual images offence shows that this high threshold limits prosecutions
- Unless reformed, this law will have almost no impact, with risk of women's faith in criminal justice system being even further undermined
- Introduce consent-based offence which is comprehensive and straightforward and forms better base for education initiatives

7. Pornography: extreme porn, incest porn and sexually violent porn easily accessible on Google, Twitter and Pornhub

- Age assurance/verification not required for Google and unclear what will be required of Twitter
- In any event, age assurance will be *easily* evaded by older children
- Importance of focussing on content of pornography
- Recognise easy availability of rape and incest porn via Google and other search engines
- Recognise Twitter hosts porn including incest porn, forced sex, cartoon child sexual abuse images, choking porn
- 1 in 8 titles on front page of mainstream commercial sites including Pornhub describe sexual violence. This is what the companies are choosing to showcase to first time users.
- Content only going to change if proactive, robust enforcement by Ofcom challenging status quo and current disregard for service providers' own terms and conditions.
- Only user-to-user and search services have duty of care and safety obligations: Important to note that while the Bill extended age assurance requirements to all porn providers, only those with user-to-user services are required to comply with the safety duties.
- Add new requirement for porn services to require verification age/consent of those in videos uploaded
- Criminalise false representations of consent when uploading porn by users

8. Mandatory Code of Practice on Violence Against Women and Girls

- Mandate Ofcom produce VAWG Code of Practice: amend Bill to mandate Ofcom to produce a Code of Practice regarding VAWG in consultation with the violence against women and girls' sector
- Revise Code of Practice for Online Child Sexual Exploitation and Abuse: revise to ensure duties of care recognise and understand gendered nature of abuse

9. Amend harm definition to recognise multiple intersecting characteristics

- *Definition of harm does not recognise intersecting characteristics:* The definition of harm in cl 187 does not appear to recognise intersecting characteristics, such as being a black woman, leading to a lack of understanding of the nature and prevalence of online harms.
- *Revise harm definition to include intersecting characteristics:* the definition of harm needs to be revised to ensure account can be taken of intersecting characteristics such as those specified in the Equality Act 2010.

Expertise

Professor Clare McGlynn QC (Hon) is an expert on laws relating to pornography, sexual violence and online abuse and co-author of the recent study revealing 1 in 8 titles on mainstream porn sites describe sexually violent porn reported in *Sunday Times* and *New York Times*. She's given oral evidence before committees of the Scottish, UK Parliament and New Zealand Parliament regarding online abuse laws, as well as oral evidence to Parliament's Joint Committee on the Online Safety Bill. She's worked with social media companies including Facebook, Google and TikTok regarding online abuse and is co-author of the recently published books *Cyberflashing: recognising harms, reforming laws* (2021) and *Image-Based Sexual Abuse: a study on the causes and consequences of non-consensual imagery* (2021). www.ClareMcGlynn.com @McGlynnClare

1. Regulation of online abuse and harms enhances freedom of speech

- The freedom of expression of many, particularly women and people from marginalized or vulnerable communities, is currently constrained and limited due to the prevalence and significant harms of online abuse.
- Women commonly self-censor online for fear of abuse and reprisals. The prevalence and harms of abuse are significantly worse for black and minorized women (Glitch and EVAW 2021).
- Debates over freedom of expression commonly assume that regulation inhibits speech and should not be adopted. But this approach fails to understand that the current position already limits the speech of women and marginalized groups.
- Better regulation of online harms and abuse, therefore, is necessary to ensure the freedom of expression of many. Regulation therefore is *human rights enhancing*.
- This was recognized by Parliament's Joint Committee on Human Rights in 2014 when it justified extreme pornography laws as 'as a human rights enhancing measure'.

2. Illegal Content Definitions and Over-Reliance on Criminal Law

2.1 Problems with using criminal law as basis for tackling violence against women and girls: In general, the criminal law was not designed and has not been interpreted with women's harms in mind. In practice, this means that, particularly regarding online abuse, the criminal law is piecemeal, incomplete, out of date and confusing. Ultimately, therefore, reliance on the *existing* criminal law as the foundation for online regulation is always going to be a partial, limited and less effective approach for women and girls.

2.2 Need to understand violence against women & girls is experienced as a continuum of abuse: This approach also assumes a hierarchy of seriousness, and separation into different incidents of abuse, which is rarely apparent in relation to violence against women and girls. Women and girls experience violence and abuse on a continuum, often experiencing many different forms of abuse, each overlapping and difficult to disentangle into specific criminal offences. There is no obvious hierarchy of abuse, as this depends on women and girls' individual experiences, often including past experiences of abuse. So-called 'minor' offences, for example, may trigger significant harms due to prior abuse.

2.3 Few bright lines between criminal and non-criminal content: The use of the criminal law as a basis for regulation assumes bright lines between criminal and non-criminal content that is rarely obvious from content alone. Criminal offences require proof of intentions and possible defences. This focus on offences detracts from a systems-based approach.

2.4 Amend definition of illegal content to be more flexible, leading to more effective regulation

Accordingly, the definition of Illegal content should be amended to providing greater flexibility and therefore ensure more effective regulation. If not, the risk is that many examples of harmful content will not be regulated by service providers. The revised definition does *not* in fact make regulation clearer (as is the aim) but *more* difficult as more detailed interpretations required.

2.5 Limits of current definition: Illegal content is defined as that which "amounts to" a "relevant offence" (cl 52(2)) which includes the priority offences listed in Schedule 7 and a fall-back category of offences comprising offences "where the intended victim is an individual". This definition seems to require the service provider to make an assessment, and to get it right, of whether an offence has been committed. This brings into play questions not just about the *nature* of the content, but also other aspects of the

offence, notably defences and the mental state (*mens rea*) of the defendant. This appears to mean that the same content may or may not fall within the regime depending on external factors such as the defendant's state of mind or having a defence. In essence, it is challenging to determine from the content of material whether a criminal offence has been committed.

2.6 Current definition may limit enforcement and regulation: This revised definition 'amounts to' does *not* make service providers' obligations clearer. In fact, it may lead to platforms refusing to act on basis content does not amount to an offence, leaving considerable gaps in protection.

2.7 Revise definition to reasonable grounds or content of a type: Instead, focus should be on requiring service providers to have systems in place to deal with types of content, *equivalent* to that which would form part of a criminal offence, were all the other elements of the offence present.

In contrast, an earlier draft Bill referred to a service provider having 'reasonable grounds to believe' an offence had been committed which granted more latitude in determining the scope of obligations, a standard more consonant with the challenges of identifying whether offences have been committed. For example, in relation to extreme pornography, different definitions would provide more useful guidance and obviate detailed discussion, complaints and legal action, such as 'content of a type likely to constitute extreme pornographic imagery' or content where 'there are reasonable grounds to believe might constitute an extreme pornographic image'.

2.8 Recommend amending definition of illegal content: amend cl 52(2) which defines illegal content as that which 'amounts to' a criminal offence to where service providers have 'reasonable grounds to believe' an offence has been committed as in an earlier draft of the bill or refer to "content of a kind' (which is used in (cl 53(4)(c) and cl 54(3)(b) respectively).

2.9 Include Scotland and Northern Ireland offences as priority offences: amend priority offences in Schedule 7 to include equivalent offences under Scots and Northern Irish law.

3. Limitations and Gaps in Priority Offences listed in Schedule 7

Extreme Pornography

3.1 Extreme pornography: varying standards across UK, with Scots law most comprehensive: The definitions of extreme pornography vary across the UK, with Scots law providing the broadest approach. Regulators, therefore, if they are to take obligations regarding extreme porn seriously, will need to use Scots law as the basis for regulation. For example, English law does not cover all forms of bestiality and only includes serious injury where that injury is to the anus breasts or genitals. See here for a more detailed analysis.

3.2 Lack of clarity on definition of 'extreme pornographic image': The definition of an extreme pornographic image requires the material to be 'obscene' which can give rise to difficulties.[1] The English Crown Prosecution Service states that 'obscene' has an 'ordinary meaning ("repulsive", "filthy", "loathsome" or "lewd")'. It is not obvious that the words loathsome, lewd and similar further any real understanding of what might constitute an 'obscene' image.[2] It is also not obvious what will constitute 'serious injury', with particular challenges around BDSM material. The English CPS guidelines simply state that the words' 'ordinary meaning' should be applied. Porn involving weapons is likely to be included (and may constitute 'life-threatening images'). Images of choking might be included.

3.3 Extreme pornography does not cover incest material: Extreme porn laws cover material depicting necrophilia, bestiality, rape and sexual penetration, life-threatening injury, or serious injuries. They do not cover material depicting incest which is common on the mainstream commercial porn sites and is easily accessible via one-click on google.

3.4 Non-consensual sharing of sexual images with intent to cause distress

The criminal offence of non-consensual distribution of private sexual images with intent to cause distress (section 33 of the Criminal Justice and Courts Act 2015) is listed as a priority offence in Schedule 7.[3]

3.5 English law motive thresholds limits prosecutions: Schedule 7 lists the English law offence which is limited in its scope and has been subject to criticism for many years. It is the subject of an on-going review by the Law Commission which was initiated three years ago in 2019. The offence only applies on proof of a perpetrator's intention to cause distress which excludes a wide range of abusive acts, including where groups of men trade and share images amongst themselves, referred to as 'collector culture'. The motive requirements in section 33 have been identified by police and victim organisations as being one of the reasons why prosecutions are so low.

3.6 English law not include deepfakes and altered/photoshopped images: Further, English law does not cover the non-consensual distribution of altered, fake images, often referred to as fakeporn or deepfakes. This is quintessentially an issue of online violence against women and girls, growing ever more common and extremely harmful.

3.7 Scots law broader: (a) definition of an intimate image includes altered images, such as deepfakes; and (b) wider range of abusive motivations, as it includes reckless intention to cause distress. Due to cl 52(12) it is Scots law that should dictate service providers obligations.

Recommendations:

3.8 Deepfake/altered images: Amend section 33 of the Criminal Justice and Immigration Act to include the non-consensual distribution of deepfake/altered images to bring in line with Scots law.[4]

3.9 Amend law on intimate image abuse: Government to commit to reviewing the law on intimate image abuse following publication of Law Commission and to swift new legislation providing a comprehensive, straightforward law, with Schedule 7 being urgently amended to include new offences.

4. Extend Schedule 7 to include more violence against women offences

4.1 Current limited scope of Schedule 7

To address violence against women and girls, the list of priority offences needs to be extended. DCMS state that the criteria used to determine inclusion in Schedule 7 include:

(a) prevalence: offences with greatest risk of harm, including the number of people likely affected;

(b) severity of harm: how severely individuals might be harmed; and

(c) ability to act: the extent to which services providers can act against the offending activities.[5]

The following offences are recommended to be included in Schedule 7 to substantiate the claim that the Bill tackles violence against women and girls. Each of the following satisfy the DCMS tests.

4.2 Trafficking and Modern Slavery Act 2015, sections 2 and 4

It is not clear why offences in the Modern Slavery Act 2015 are not included, especially as the role of social media and other service providers in facilitating such abuse has been consistently highlighted. It is particularly unclear why the offence of assisting unlawful immigration is included in Schedule 7, an offence where the 'victim' is the state, but not the trafficking offences where there are potentially thousands of individual victims. Include s2 - arranging or facilitating the travel of another person with a view to exploitation and s4 - committing an offence with intent to commit an offence under section 2 of the Act.

(a) *Prevalence:* The 2021 Independent Review of the Modern Slavery Act estimated that 10-13,000 victims of modern slavery in the UK, with some figures suggesting considerably higher prevalence.
(b) *Severity of harm:* potentially life-threatening and life-long trauma including sexual exploitation and violation. The Impact Assessment for the Bill estimates that modern slavery costs approximately £10.7 million a year, and this figure is based on criminal justice statistics and therefore the actual cost is likely to be considerably higher.
(c) *Ability of service providers to act:* Social media and service providers could take far greater action to disrupt trafficking, as identified in the leaked Facebook files.

4.3 Cyberflashing, cl 156 of the Bill

This is quintessentially an online harm and sufficiently serious to be included in the Bill as a new offence in cl 156 (and included in s2 of the Justice (Sexual Offences and Trafficking Victims) Act (Northern Ireland) 2022).

(a) *Prevalence*: Cyberflashing is alarmingly common with approximately half of young women having been sent penis images without their consent, rising to three-quarters of under-18s.
(b) *Severity of harm*: cyberflashing can be threatening, intimidating and experienced as a serious sexual violation. It can have life-threatening impacts, as seen in recent Gaia Pope case.
(c) *Ability to act:* Service providers could be taking far greater action against cyberflashing, as exemplified by the technology developed and used by Bumble to block penis images. Other platforms are failing to take robust action against cyberflashing, with Instagram for example refusing to remove such material saying it does not violate their guidelines.

4.4 Blackmail (sexual extortion) - s21 of the Theft Act 1968

Sexual extortion (sextortion or webcam blackmail) is committed online, can be potentially life-threatening and, when committed against adults, the motivation is predominantly financial. Sexual extortion against children is predominantly for sexual gratification. Sextortion is a form of image-based sexual abuse, similar to non-consensual distribution of sexual images which is a priority offence listed in Schedule 7. While sexual extortion can include a number of criminal acts, sexual extortion for financial gain is prosecuted via s21 of the Theft Act 1968.

(a) *Prevalence:* sextortion has surged since covid, with police receiving more than 9000 reports in the six weeks leading to May 2020.
(b) *Severity of harm:* sextortion can be life-threatening, with many reported suicides, and it is commonly experienced as devastating and violating.
(c) *Ability to act:* as with all forms of image-based sexual abuse, social media and service providers could be taking much stronger action to disrupt extortion via their platforms, and to take action when notified of extortion cases and materials.

4.5 Obscene Publications Act 1959, s2

Section 2 of the 1959 Act criminalises the publication (whether or not for gain) of an 'obscene' article and therefore specifically addresses the distribution of a pornographic materials deemed unlawful. This is, therefore, a provision pre-eminently appropriate for Schedule 7, particularly in view of Government's expressed concern about unlawful pornography. There is overlap between obscenity and extreme pornography and the boundaries are unclear. However, it is possible that the following types of material may be classed as obscene, but not extreme porn:

- *bestiality*: masturbation of or by an animal as there is no consent (extreme porn only covers penetration or oral sex) (though Scots law on extreme porn covers this activity)
- *Incest porn:* depictions of acts which constitute criminal offences, such as penetrative sexual activity between proscribed family members including parents, children, aunts and uncles.
- *serious bodily injury*: pornographic material depicting serious injury to the body other than the anus, breasts or genitals where such acts may constitute criminal conduct (some such material may be covered in Scots law on extreme porn)
- *choking and suffocation:* depictions of choking and suffocation might be considered 'life-threatening' and if so, may constitute an extreme pornographic image. If not, they might be considered actual bodily harm and therefore criminal conduct and potentially obscene.
  (a) *Prevalence*: There is an extensive amount of incest material online, including on the mainstream commercial pornography websites and it is easily available on Google.
  (b) *Severity of harm:* Incest material, in particular, minimises and normalises abusive sexual activity, including sexual interest in children.
  (c) *Ability to act:* service providers could take significant steps to reduce obscene materials online. Even acting on the simplest word searches could reduce the prevalence of incest material.

5. Extend Schedule 6 to include more child sexual offences

5.1 Schedule 6 includes range of child sexual offences*:* Schedule 6 lists a range of child sexual offences in the Sexual Offences Act 2003 (including equivalents across the UK) including the grooming offences, child sexual exploitation (prostitution) offences, as well as the offences in sections 8-13 relating to causing or inciting children to engage in sexual activity, causing children to watch sexual acts and child sexual offences committed by young people. While many of these offences can be directly committed using online technology, such as grooming offences, the list also includes offences that can be committed in person and physically, such as s13 which criminalises young people engaging in sexual activity with a child.

5.2 Unclear why some child sexual offences not included: However, it is not clear why some sexual offences are included but not others, including offences involving breach of a position of trust (s17 causing or inciting a child to engage in sexual activity when in a position of trust; s18 (sexual activity in the presence of a child when in a position of trust) or s26 (inciting a child family member to engage in sexual activity). In terms of maximum terms of imprisonment, the abuse of trust and familial provisions are not as serious as some other child sexual offences, but this does not appear sufficient reasons to exclude them. These are also offences that can be committed online, as they involve incitement which can be via text, video or similar.

5.3 Recommend: including sections 17, 18 and 26 in Schedule 6 (and Scottish equivalents).

6. Amend Cyberflashing offence to be comprehensive and consent-based

6.1 Summary

- Welcome proposal to introduce new offence criminalising cyberflashing in light of significant evidence of potential harms.
- However, cl 156 is a limited and partial response to calls to criminalise all forms of cyberflashing.
- Cl 156 (a) does not cover all forms of cyberflashing and (b) introduces motive threshold that will make prosecutions difficult, as seen with law on non-consensual distribution of sexual images.
- Unless amended, the law will have little practical effect.
- Recommend amending cl 156 to a consent-based offence which is comprehensive, straightforward and follows best practice from the United States.
- For more detailed justification of consent-based law, see McGlynn, 'Cyberflashing: consent, reform and the criminal law' (2022) *Journal of Criminal Law*
- For a short blog on problems with motive-based offence, see A proposed new law criminalising cyberflashing is welcome – but it has one major flaw | The Independent
- This evidence draws on my recently published co-authored book *Cyberflashing: recognising harms, reforming laws* (2021) which is the most comprehensive study of cyberflashing internationally to date. A summary of the research findings and recommendations is available here.

6.2 Law reform options

There are two main options when drafting a new cyberflashing criminal offence:

- a comprehensive 'consent-based' offence requiring proof of non-consent; or
- a limited 'motive-based' offence, as proposed in section 156 of the Online Safety Bill, where there is only a criminal offence on proof of specific motives of the offender, such as causing distress, alarm or humiliation, or sexual gratification and being reckless as to causing distress.

6.3 Justifications for consent-based cyberflashing offence

6.4 No evidence that only certain motives cause harms of cyberflashing

- Men's motivations for cyberflashing are varied and overlapping and include misogyny, causing distress, sexual gratification, humour, boosting status amongst peers and transactional (to get nudes in return).
- There is *no evidence* that harms experienced by women are worse when offenders are motivated by the specific purposes identified in 'motive-based' proposals: eg a woman on public transport may feel threatened when sent unsolicited penis images, regardless of whether the sender intended to cause alarm or as 'banter' amongst friends.

6.5 Men most commonly send penis images for reasons *other than* those in cl 156

- Research finds that men commonly send penis images as a way of 'showing off, complimenting, hooking up with or getting nudes in return'.
- Another study found that 77% sent images in hope of getting nudes in return or meeting up in real life.
- Only 18% sent images for sexual gratification and only 15% for reasons of power, control, to cause distress.

- Government media justified new cyberflashing law referring to study finding 76% of teenage girls have been sent unsolicited penis images. Yet, in vast majority of these cases, the motive thresholds will not be satisfied as they are not sent to cause distress, but mostly to gain nudes in return or to show off.
- The majority of cyberflashing cases may not be included within this offence – yet the media rhetoric suggests otherwise.

6.6 MOJ misunderstands motives by claim police won't take 'banter defence' at face-value

- MOJ defend the motive-based offence on the basis that police will not take 'joke/banter' defence at face value and will investigate.
- This misunderstands motives as this is in fact why some men send penis images; it's not just a 'defence', but the harm experienced can be considerable. It means these cases will not be prosecuted as there will be no evidence to support prosecution.

6.7 MOJ relies on outdated investigation practices to defend motive-based approach

- MOJ defend the motive-based offence stating the focus is on the perpetrator, whereas consent laws (like rape) focus too much on the victim.
- It is true that *existing* approaches to investigation and prosecution of rape focus too much on the complainant, and not on what actions the perpetrator took to obtain consent. However, it is this problematic approach which has been identified as in need of reform, hence why the Government has invested millions in Project Soteria Bluestone to reform police investigations.
- The law should not be introduced on the basis of *already established bad practices*.
- Police should focus on steps a perpetrator took to ensure consent and expect evidence. It must be remembered that seeking consent is straightforward – they just have to ask if someone wants to see a penis image.

6.8 Motive requirements will limit police investigations and prosecutions

- Evidence to support the motive needs to be secured, requiring additional time, effort and resources. We know from police and victims that investigations and prosecutions for sharing sexual images without consent (often problematically referred to as 'revenge porn') are not taken forward due to similar motive requirements. The Revenge Porn Helpline report that the distress motive requirement hinders prosecutions.

6.9 Consent should be the focus of prevention and education initiatives

- A consent-based offence provides a better foundation for education and prevention. It sends the message that all sexual activity should be grounded in consent including all online activities, and that *any* taking or sharing of sexual images without consent is wrong, harmful and criminal.

6.10 Consent-based law follows international best practice

- A consent-based cyberflashing offence has been adopted in Texas and is being debated in other US states.

6.11 Consent is easily obtained and criminal charges easily avoided

- It is important to remember that avoiding being charged with a criminal offence is straightforward: all the sender needs to do is ask, would you like to see a picture of a penis?

6.12 Motives not required for most criminal offences including sexual offences

- Most criminal offences do not require proof of specific motives. The criminal law is generally concerned with an individual's intention to carry out the particular act (eg assault someone) rather than *why* they have done it. The why (motive) becomes relevant in gathering evidence and sentencing,

but not as an element of the crime itself. In the Sexual Offences Act 2003, three-quarters of offences do not require a motive. Proof of a 'guilty mind' (*mens rea*) is still required in a consent-based offence: proof of intention to distribute a penis image without consent and no reasonable belief in consent. It is *not* a strict liability offence.

6.13 Young men and 'over-criminalisation'

- We must not unduly criminalise young men sending penis images. As with other offences, prosecution guidance and schools' guidance determine when it is and is not appropriate to investigate and intervene.
- Education is critical to changing behaviours – but this education should be based on *consent* as being the foundation for all sexual activity.
- Laws determining adult behaviour should not be re-framed based on applicability to children.
- While there are legitimate debates about over-criminalisation in general, it is important to note that women's experiences of online abuse are *under-criminalised*.

6.14 Consent prioritises protecting girls from harassment over boys 'misguided' humour

- The proposed cyberflashing offence is based on Law Commission proposals which justify a motive-based offence as it excludes the 'juvenile' who sends penis images in a 'genuine (even if misguided) attempt at humour'. However, hateful or racist speech may be deemed funny by perpetrators, but the humour motive does not insulate them from prosecution.
- Young boys may send penis images as a joke or to gain nudes in return which they then use to boost their status amongst their peers. Teenage girls commonly experience being sent penis images as coercive; some also experience harassment simply as a result of being sent the images.
- If this scenario is used to justify a motive-based offence, the law will be prioritising boy's attempts at 'misguided' humour, over girls' experiences of relentless harassment. It would mean that most teenage girls' experiences will fall outside of the law. All boys have to do is ask and seek consent.

6.15 Proposed amendment to cl 156:

New text in italics.

In the Sexual Offences Act 2003, after section 66 insert—

"66A Sending etc photograph or film of genitals

(1) A person (A) who intentionally sends or gives a photograph or film of any person's genitals to another person (B) commits an offence if –

(a) B does not consent to the sending or giving of the photograph or film, and

(b) A does not reasonably believe that B consents.

(2) Whether a belief is reasonable is to be determined having regard to all the circumstances, including any steps A has taken to ascertain whether B consents.

~~*(a) A intends that B will see the genitals and be caused alarm, distress or humiliation, or*~~

~~*(b) A sends or gives such a photograph or film for the purpose of obtaining sexual gratification and is reckless as to whether B will be caused alarm, distress or humiliation.*~~

7. Pornography: extreme porn, incest porn and sexually violent porn easily accessible on Google, Twitter and Pornhub

7.1 Pornography is regulated in the Bill in two main ways:

- Age assurance/verification, restricting access by children; and
- Content regulated via duties of care, particularly priority offences.

Age assurance will be easily evaded by older children

7.2 Ease of evading age assurance: Survey evidence suggests that 46% of 16–17-year-olds have used a VPN or Tor browser, and another 23% knew what they were. This means that older children may be able to evade age restrictions with relative ease.

7.3 Efficacy of age assurance obligations on pornography services: It should also be noted that even if age assurance provisions are enacted, implementation is not guaranteed. Experience so far from France and Germany shows that despite legal requirements to introduce age restrictions and pressure from regulators, pornography platforms are strongly resisting and are not acting, including Pornhub, despite it publicly stating its support for age verification. While there are enforcement mechanisms in the Bill, including business disruption measures and fines for executives, regulatory enforcement will be a challenge due to the lack of transparency regarding the ownership and control of the largest pornography platforms.

7.4 Recommend harmonizing age assurance/verification requirements: The specific requirements on user-to-user and other porn service providers are not the same and regulation would be easier if they were harmonized. See cl 68(2) regarding provider porn and cl 31(2) for user-to-user services.

7.5 Importance of focusing on content of mainstream pornography: While age assurance regulations dominate public discussion regarding pornography and the Bill, the reality is that, were it not for the problematic nature of much mainstream pornography, and the impact of business and service design on user-generated content, there would be far less concern regarding children's access. Therefore, where a key aim is to reduce the adverse impacts of pornography on children, a dual approach is required, tackling content *and* access.

Focus on content

7.6 Easy availability of sexually violent pornography via Google and mainstream porn sites

7.7 Rape porn and incest material easily and freely available via search services like Google: a one-click search on Google brings up pages and pages of rape porn content featuring incest, weapons, teenagers and racialised titles, with links to dedicated rape and forced sex pornography websites. The easy availability of rape porn contributes to a climate where sexual violence is normalised and minimised. Incest material is similarly available with one-click. This is not in the dark recesses of the internet where you have to be very determined to find material.

7.8 Mainstream commercial porn sites choose to show sexually violent porn to first-time users: My recent research with Fiona Vera-Gray and others found 1 in 8 video titles advertised to first-time user – ie young and teenage boys - on UK's most popular porn websites describe acts of sexual violence. Material depicting criminal acts such as rape, incest and upskirting are being actively pushed to the front page by the porn companies, in direct contravention of their own terms and conditions.

7.9 Extreme pornography: Schedule 7 only includes the extreme pornography offence. The scope of this offence is not as obvious as might be thought, potentially giving rise to regulatory challenges (eg grounds for obfuscation from service providers) and highlights the problem of focussing on specific criminal offences for regulating content. For example, the image has to be classed as obscene which is not a clearly defined term. This means that porn services will be obligated to ensure this material is not on their services and swiftly remove any such content.

7.10 Prevalence of image-based sexual abuse on porn sites: Obliging porn platforms to act in relation to intimate image abuse material, often called non-consensual pornography, is vital due to the prevalence and harms of this material. The Revenge Porn Helpline reports that the main destination for distribution of non-consensual material is pornography websites, making up 52% of reports to their service. Notably this is an *increase* in material being distributed on porn sites from previous years. Other research with victims found that 1 in 5 had their images distributed onto pornography websites.[6] Analysis of the content of mainstream pornography websites found many titles suggesting non-consensual porn on the landing pages of the websites. Many victims have spoken out about their experiences of having sexual images of them shared on porn websites and their difficulties of getting the material removed.[7] Investigations by the *New York Times* also revealed the easy availability of unlawful material that had been circulating on mainstream porn sites for many years, despite attempts to get it removed.[8] For example, the recent study of the content of mainstream porn sites found titles such as 'Cheated GF fucked on webcam in revenge porn'. However, it should be noted that the terms and conditions of such porn providers have long stated that they do not to allow non-consensual material on their sites, yet the material is still available online, despite being so easily identified by simple word searches. It has been argued such T&Cs are 'works of fiction'. The safety duties require services to enforce their terms of service consistently; it is unclear whether this allows equally poor non-enforcement.

How will the Bill affect services providing porn?

7.11 Google – search service with easily accessible extreme pornography

The easy availability of rape pornography via one-click on Google provides a clear example of how easy it is to access material that is unlawful to possess or distribute, and which plays a significant role in normalizing and minimizing sexual violence.

7.12 Children's access: As the service is a search service and not a provider of porn, it is not affected by the Part 5 children's access obligations.

***7.13 Children's duties of care*:** Google is a service likely to be classed as 'likely to be accessed by children' and therefore child safety duties apply. These require a search service to minimise the risk of children in age groups judged to be at risk of harm from encountering search content that is harmful (including pornography which is priority content). However, the obligation is to 'minimise' risks and harms and may be satisfied by means such as parental controls.

7.14 Other duties of care: Google will be required to undertake a risk assessment including identifying the level of risk of encountering priority illegal content, such as extreme porn, as well as identifying the nature and severity of harm that might be suffered. There is a very high level of risk of encountering extreme porn (and other illegal porn) through search on Google, and the harm is considerable (hence why the possession of this material is a criminal offence).

7.15 Will anything change? The duty of care applying to priority offences, such as extreme pornography including rape porn, *should* make a considerable difference to searches on Google. However, key will be whether Ofcom accepts a minimal approach reliant on safe search and parental controls as satisfying the safety duty. If it does, little will change and extreme porn will be easily accessible via Google, without the need to evade age verification controls on porn sites.

7.16 Pornhub and similar large, mainstream commercial porn services

Age assurance/verification will be required. Note however that this is easily evaded, including by using the porn providers own specifically created VPN apps.

Safety duties will apply to any user porn, but *not* porn provided by the porn service. Any service that only showcases provider porn is *not* affected by the safety duties.

7.17 Extreme porn and some non-consensual porn: Service providers will have to take steps to prevent users encountering this priority content and reduce the time it's available.

7.18 Duty regarding obscene materials: This is only classed as illegal (non-designated) content and service providers are only obliged to 'mitigate and manage' risks. Theoretically, this should mean service providers might remove material when identified.

7.19 Will anything change? Age assurance/verification will be required (though easily evaded). While new illegal content duties *could* impact on the content available, there are unlikely to be any significant changes regarding content unless there is proactive investigation and challenge from Ofcom, due to these services currently failing to comply with their own terms of service and obfuscating attempts to remove unlawful content.

7.20 Twitter: user service with porn content, likely accessed by children

7.21 Availability of pornography: Twitter is an example of a user-to-user service where user-generated pornography can be easily accessed, including material advertised as incest, cartoon child sexual abuse material (that falls short of laws on prohibited images), forced sexual activity and choking.

7.22 Children's access and duties of care: As Twitter only displays user-generated porn, the access restrictions in Part 5 of the Bill do not apply. Platforms providing user porn only, such as Twitter, will be subject to the general children's safety duties as they are likely to be accessed by children (unless they put in place measures to ensure that children do not access the service (cl 31(2)).

***7.23 Children's duties of care*:** As the Government has indicated that all pornography will be classed as 'priority content' regarding children, this would require Twitter to protect children in age groups judged to be at risk of harm from encountering this content, for example by using age assurance mechanisms.

7.24 Other duties of care: This will principally mean ensuring no extreme porn on the service. More challenging will be obligations to ensure that some forms of non-consensual sexual material listed as priority offences are not encountered through the service, and to take down that content swiftly on becoming aware of it. In relation to other illegal pornography, such as obscene materials, there are reduced obligations, such as having a system to remove such content when notified.

7.25 Will there be any change following the Bill?: As pornography is likely to be classed as 'priority content' regarding children, this *should* require Twitter to protect children in age groups judged to be at risk of harm from encountering this content, for example by using age assurance mechanisms. It is unclear exactly what will be required to meet this obligation. Will Ofcom consider the option to restrict sensitive content enough?

7.26 OnlyFans: user to user service with porn content

OnlyFans is an example of a user-to-user service displaying pornography. The extent of its obligations will depend on whether it is classed as a service 'likely to be accessed by children' and, if so, it will have to put in place age assurance/verification. While the service is aimed at over 18s, recent investigations have shown how easy it has been for children to establish accounts.

7.27 Change following the Bill?: As OnlyFans is based on user-generated material over which the content creators have control, there is far less scope for unlawful and harmful material on the service. As the Bill largely focuses on criminal content (regarding adults), the Bill will likely have little impact on the content available on the site. Far more of an issue is the use of content creators' pornographic material without their consent, such as pornography unlawfully downloaded from OnlyFans and distributed on other porn services and forums.

7.28 Bill amendments to limit distribution of intimate images without consent by porn services

Consideration should be given to the following measures which would aim to reduce the extent of unlawful material on pornography services:

7.29 Require porn companies to verify the age/consent of all those in pornographic videos/images

- The Online Safety Bill could include new provisions requiring pornography providers to ensure the age and/or consent of all those featured in provider porn and user porn that is published or displayed on their sites.
- Such a provision was by the Canadian Parliament's Standing Committee on Access to Information, Privacy and Ethics in June 2021: 'That the Government of Canada mandate that content-hosting platforms operating in Canada require affirmation from all persons depicted in pornographic content, before it can be uploaded, that they are 18 years old or older and that they consent to its distribution, and that it consult with the Privacy Commissioner of Canada with respect to the implementation of such obligation.' [9]
- These provisions are now included in a Private Member's Bill currently before the Canadian Parliament.[10]

7.30 New offence criminalising the individual user who makes false representations of consent when uploading to porn websites

- The Online Safety Bill could Introduce a new criminal offence where an individual user makes a false representation that they have the consent of all those featured in any user porn to be uploaded to a service provider.
- This has been recommended by a coalition of violence against women organisations in their evidence regarding the Online Safety Bill. Such a provision would mirror current laws where making false representations can constitute the criminal offence of fraud.[11]
- A similar provision was recommended by the Canadian Parliament's Standing Committee on Access to Information, Privacy and Ethics in June 2021: 'That the Government of Canada set requirements for uploaders of content to provide proof of valid consent of all persons depicted and that the new regulations include penalties severe enough to act as an effective deterrent.'

8. Violence against Women and Girls Code of Practice

8.1 Code will help ensure service providers take violence against women and girls seriously

Without VAWG being clearly identified as a priority harm, and with only a limited range of offences listed as priority offences, it is vital that more steps are taken to ensure service providers take violence against women and girls seriously. This requires an in-depth understanding of the specific nature of online VAWG as it is different in its manifestations, extent and harms.

A coalition of groups – EVAW, NSPCC, 5Rights, Glitch, Refuge, Lorna Woods and Clare McGlynn – have prepared a draft Code of Practice which demonstrates what is possible.

It also requires an intersectional understanding as A Code can also help ensure Without a specific Code of Practice regarding online VAWG, the risk is that the specific context and nature of such abuse is not recognised by platforms and action is not taken, even if VAWG is defined on the face of the legislation.

Recommendation:

8.2 Mandate Ofcom produce VAWG Code of Practice: Amend Bill to mandate Ofcom to produce a Code of Practice regarding VAWG in consultation with the violence against women and girls sector, specifically including organisations working with black and minoritised women such as Glitch, Imkaan and the Angelou Centre.

8.3 Revise Code of Practice for Online Child Sexual Exploitation and Abuse: The current draft Code of Practice for Online Child Sexual Exploitation and Abuse fails to identify the specific nature, extent and harms experienced by girls. This is glaring omission in view of the gendered nature of child sexual abuse and exploitation. There is no recognition of multiple and intersecting identities meaning that there is no consideration of, for example, the particular experiences of young black girls, or those identifying as LGBTQI. A revised Code covering these issues is vital if it is to provide effective guidance to regulated services in carrying out their risk and safety duties.

9. Amend definition of harm to ensure intersectional approach

9.1 Harm affecting 'appreciable' number of people and intersecting characteristics:

Content that is harmful to children or harmful to adults is either content listed as priority content or is defined as "content of a kind which presents a material risk of significant harm to an appreciable number" of children or adults in the UK (cl 53(4)(c) and cl 54(3)(b) respectively).

By referring to the population of the UK as a whole, this definition does not acknowledge that some groups are both more likely to be harmed by certain types of material and more likely to encounter it. For example, black women are disproportionately affected by online abuse and targeted for that abuse due to being both black and a woman (sometimes referred to as misogynoir).

However, whether the harms to black women are 'significant' to an "appreciable number" of adults in the UK is not clear and the risk is that they are not.

9.2 Harm definition not clearly acknowledge linked characteristics, eg being a black woman:

"Harm" is defined as "physical or psychological harm" (cl 187(2)). Clause 187(4) recognises that harm may arise where individuals do or say something as a result of content that is 'related to the other person's individual characteristics or membership of a group'. However, the language used implicitly assumes that there will be a single characteristic defining the group, and thus does not deal with intersecting

characteristics, for example racism and sexism. This is a significant gap as, for example, black and minoritised women experience online abuse, and at disproportionate levels, based on being black/minoritised *and* a woman.

9.3 Definition of harm does not recognise intersecting characteristics: The definition of harm in cl 187 does not appear to recognise intersecting characteristics, such as being a black woman, leading to a lack of understanding of the nature and prevalence of online harms.

9.4 Revise harm definition to include intersecting characteristics: the definition of harm needs to be revised to ensure account can be taken of intersecting characteristics such as those specified in the Equality Act 2010.

---

[1] For an analysis of the extreme pornography offence, data on prosecutions and recommendations for reform, see Clare McGlynn and Hannah Bows, 'Possessing Extreme Pornography: Policing, Prosecutions and the Need for Reform' (2020) 83(6) *Journal of Criminal Law* 473-488 and Clare McGlynn and Erika Rackley, Criminalising Extreme Pornography: A Lost Opportunity (2009) *Criminal Law Review* 245-260.

[2] To further confuse, there is no symmetry between the meaning of 'obscene' in the extreme pornography offence (a lower threshold based on the 'ordinary' meaning of the word) and obscenity under the Obscene Publications Act (meaning the actions must also 'deprave and corrupt'). For an explanation and discussion, see Clare McGlynn and Hannah Bows, 'Possessing Extreme Pornography: Policing, Prosecutions and the Need for Reform' (2020) 83(6) *Journal of Criminal Law* 473-488.

[3] The Government problematically describes this offence as 'revenge porn', Government Press release, 4 February 2022: Online safety law to be strengthened to stamp out illegal content - GOV.UK (www.gov.uk). For a short blog on the problems with terminology 'revenge porn', see Clare McGlynn and Erika Rackley, Not 'revenge porn', but abuse: let's call it image-based sexual abuse by @McGlynnClare & @erikarackley | Everyday Victim Blaming and Clare McGlynn and Erika Rackley, 'Image-Based Sexual Abuse' (2017) 37 *Oxford Journal of Legal Studies* 534-561.

[4] This is straightforward. Scots law provides a definition of intimate image or video as including material 'whether or not the image has been altered in any way' (section 3(2) Abusive Behaviour and Sexual Harm Act 2016.

[5] As indicated in the Online Harms White Paper Full Government Response to Consultation, December 2020, para 2.20 and in DCMS briefings.

[6] Survey of 6,109 participants across Australia, New Zealand and the United Kingdom: Henry, McGlynn et al, *Image-Based Sexual Abuse: a study on the causes and consequences of non-consensual sexual imagery* (Routledge, 2021), p 29.

[7] #NotYourPorn Is The Campaign Fighting To Get Non-Consensual Content Removed From UK Porn Sites (bustle.com) and Pornhub: The ongoing revenge porn investigation (openaccessgovernment.org).

[8] Opinion | The Children of Pornhub - The New York Times (nytimes.com) and Opinion | Why Do We Let Corporations Profit From Rape Videos? - The New York Times (nytimes.com).

[9] Standing Committee on Access to Information, Privacy and Ethics, *Ensuring the Protection of Privacy and Reputation on Platforms Such as Pornhub* (July 2021): 'Recommendation of the Canadian parliament concerning the duty to verify age and consent: That the Government of Canada mandate that content-hosting platforms operating in Canada require affirmation from all persons depicted in pornographic content, before it can be uploaded, that they are 18 years old or older and that they consent to its distribution, and that it consult with the Privacy Commissioner of Canada with respect to the implementation of such obligation.'

[10] Bill C-302 432 An Act to amend the Criminal Code (pornographic material) | Projet de loi C-302 432 Loi modifiant le Code criminel (matériel pornographique) (parl.ca)

[11] Fraud Act 2006 Fraud by false representation is when someone dishonestly makes an untrue or misleading representation with the intention of making a gain for himself or causing loss to another. There are many other false representations provisions, such as in electoral laws. They usually are targeted at individuals seeking obtain financial or similar gains.