Women and Equalities Committee

3 December 2024

Dame Melanie Dawes
Chief Executive
Ofcom

Non-consensual intimate image abuse

Dear Dame Melanie,

The Women and Equalities Committee is conducting an inquiry into non-consensual intimate image (NCII) abuse.

On 20 August, the Women and Equalities Committee heard oral evidence from the Parliamentary Under-Secretary of State at the Home Office, Jess Phillips, and the Parliamentary Under-Secretary of State at the Ministry of Justice, Alex Davies-Jones. During that session, the role of Ofcom and duties under the Online Safety Act were discussed. I am writing to seek clarification from you on a number of points.

Ofcom's enforcement powers against non-compliant websites hosting NCII

We have heard evidence from the Revenge Porn Helpline (RPH) that they have a takedown rate of over 90% of the images that they report to platforms as constituting NCII. The remainder are often hosted on websites based outside of Europe, whose entire business model may be predicated on hosting NCII content.
These sites do not engage with the RPH, who currently lack any mechanism of disrupting or blocking access to such sites.

We asked Minister Davies-Jones what she would advise someone whose intimate images were being hosted on one such non-compliant website to do: her response was "until the Online Safety Act is implemented, there is no way of getting that material taken down".

However, the Committee has received evidence that Ofcom's powers under the OSA are "not designed to provide individuals with redress" and "inadequate to respond to the need for thousands of images, across many websites to be removed". We have heard that the use of business disruption orders - that Ofcom's powers include – is designed to be exceptional.

House of Commons
Palace of Westminster
London
SW1A 0AA

womeqcom@parliament.uk
+44 (0)20 7219 4432
Social: @houseofcommons
parliament.uk

We have also heard that the process that must take place before utilising them is lengthy and bureaucratic, an issue exacerbated by the fact that the NCII content may then be uploaded to a different non-compliant website, and the long process would have to restart. Yet victims of NCII have emphasised to us that their utmost priority is to have the offending content removed as quickly as possible.

I would be grateful if you could clarify:

- Given that it is not possible to submit individual complaints about NCII content being hosted on non-compliant websites to Ofcom, what are the pathways that would lead to Ofcom taking enforcement action against these sites?
- How long might engaging in such enforcement action reasonably take?

  For example, how long could it feasibly take before Ofcom could utilise its enforcement powers against a non-compliant website that hosted NCII content? Ofcom officials have previously indicated that they are unable to specify the above because the time taken for enforcement action would be "case-specific", but the Committee would like to know a general timeframe – would such action against a website based in Russia that is dedicated to hosting NCII content, for example, take days, weeks, months or years?

Service provider obligations regarding NCII and CSAM (child sexual abuse material)

The RPH has been told by internet service providers (ISPs) that they are unable to block access to NCII URLs, as doing so would risk censoring the internet to non-illegal content. The RPH has therefore urged that NCII content be classed as illegal content in the same way that CSAM is.

The Committee understands that, while the act of sharing intimate images without consent is prohibited conduct (i.e. the behaviour is 'illegal'), unlike CSAM, the criminal legislation does not make the content (the actual images/videos) illegal in and of itself. When the Committee raised the issue of giving NCII the same illegal status as CSAM, the Ministers replied that this was already the case. Minister Davies-Jones said:

> *"It is illegal. We need to be clear here that non-consensual intimate imagery that is uploaded is illegal... platforms will have to act—as if it were CSAM—to remove this content."*

Google told our Committee that making NCII illegal in the same way as CSAM would change the way they dealt with the content, in that they would remove search results

containing NCII rather than downrank them. When we put this to Minister Phillips, she replied:

> *"All I would say back to them is that it is illegal. Intimate image abuse is illegal… Terrorism, child abuse and sharing of intimate images have the same level in the Act."*

I would be grateful if you could provide clarification on the following:

- Will search engines be required to delist NCII content, as is the case with CSAM?
- Will ISPs be encouraged to block access to NCII content hosted overseas, as is the case with CSAM?
- What are the differences, if any, in how User-to-User services should treat NCII versus CSAM according to Ofcom's guidance?

  [For example, the Committee understands that it is technically possible for two different services providers to take different views on whether or not an item of content meets the threshold of 'reasonable grounds to infer' that a criminal offence has taken place in relation to that content. Theoretically, this could result in a victim being faced with two platforms making different decisions, which would not happen in relation to CSAM]

The Committee is keen to publish its report on this issue as soon as possible. I would appreciate your response to the above questions by 13 December.

A copy of this letter and your reply will be placed in the public domain.

Yours sincerely,

Sarah Owen MP
Chair, Women and Equalities Committee

House of Commons
Palace of Westminster
London
SW1A 0AA

womeqcom@parliament.uk
+44 (0)20 7219 4432
Social: @houseofcommons
parliament.uk

CONFIDENTIAL

Dame Melanie Dawes
Chief Executive
Email: chiefexecutive@ofcom.org.uk

17 January 2025

Sarah Owen MP
Chair, Women and Equalities Committee
House of Commons
Palace of Westminster
London
SW1A 0AA

Dear Ms Owen,

Non-consensual intimate image abuse

Thank you for your letter of 3 December 2024, setting out some questions that have arisen during the Committee's inquiry on non-consensual intimate image abuse ("NCII").

This is an important issue and my colleagues have compiled a technical note with responses to your specific questions – this is attached.

You may also be interested in an update on a wider progress in implementing the Online Safety Act. I have also attached the letter that I sent to Parliamentarians in December last year setting out our progress and implementation plans. We published our final Illegal Harms Codes in December last year, with measures to tackle illegal content including NCII which is a priority offence. This publication also started the clock on services taking action with the requirement to undertake an assessment of risk on their services by 16 March.

I hope this further information is helpful to the Committee as it finalises its report. My colleagues and I look forward to reading the report when it is published, and to continuing to work with the Committee.

I note your intention to make our correspondence public. I am copying this letter to the Department for Science, Innovation and Technology, to the Home Office, and to the Ministry of Justice.

Yours sincerely,

Melanie Dawes

Melanie Dawes
Chief Executive
ChiefExecutive.ofcom.org.uk

16 December 2024

The Rt. Hon the Baroness Stowell of Beeston
Chair, Communications and Digital Select Committee

House of Lords, London, SW1A 0PW

Chi Onwurah MP
Chair, Science, Innovation and Technology Committee
House of Commons, London, SW1A 0AA

Josh Simons MP
Chair, Digital Regulation and Responsibility APPG
House of Commons, London, SW1A 0AA

By email only

Online Safety Act – Publication of Illegal Harms Statement

Today Ofcom has published our Illegal Harms Statement, which marks a major milestone in the implementation of the Online Safety Act. The statement comprises Illegal Content Codes of Practice for user-to-user services and search services ("Illegal Harms Codes") and several pieces of complementary Guidance.

This means that from today, service providers will have to take actions to start complying with the new rules. The first step is the completion of illegal harms risk assessments, a new duty under the Act and a step which every provider must take by 16 March. The Government has today laid the Codes in Parliament and after they have been approved by Parliament, providers will then need to take the measures set out in our Illegal Harms Codes, or other measures which meet their duties, to protect users from illegal content and activity.

The Government has also laid the draft regulations to establish categorisation thresholds following on from Ofcom's advice earlier in the year. Once the regulations have been approved by Parliament, Ofcom will formally request information from services to inform the register of categorised services, which will be published in summer 2025.

Illegal Harms Codes

The Online Safety Act requires online services that host user-generated content and search services to protect their users from illegal harms. This includes terror, illegal hate, fraud, grooming of children, and sharing of illegal intimate images and Child Sexual Abuse Material.

Parliament set a clear priority for Ofcom in the Act, requiring us to bring the Illegal Harms Codes and Protection of Children Codes into force within 18 months of Royal Assent, which took place on 26 October 2023. In early November 2023 we launched our first major consultation, on the Illegal Harms Codes and associated guidance. With the finalisation of these Codes today, we have met the first stage of Parliament's deadline and are on track for the provisions to come into force early next year.

The Illegal Harms Codes are accompanied by seven other regulatory documents which will help guide services on how to meet their new illegal content duties. These are Ofcom's register of risk; Ofcom's risk profiles; risk assessment guidance; illegal content judgements guidance; and guidance on enforcement, record keeping, and on when content can be said to be communicated publicly.

What will change?

The documents we are publishing today are an important step toward creating a safer life online for adults and children across the UK. Taken together, the measures we are introducing set new standards and clear expectations for the industry. Some of them apply to all providers, and others to the providers of larger or riskier services.

Some of the most important changes we expect our Codes and guidance to deliver include:

- **Putting managing risk of harm at the heart of decisions.** From today, every site and app in scope of the Online Safety Act will need to complete a "suitable and sufficient" risk assessment. This means they need to assess the risks that illegal harms pose to users on their service and consider how best to tackle them. To ensure clear accountability, each provider must name a senior person responsible for illegal harms.
- **Better protections from the full range of Illegal Harms**. Providers will need to take down illegal content of all types and maintain appropriately resourced and trained content moderation teams. Reporting and complaints functions will be easier to find and use, with appropriate action taken in response. Relevant providers will also need to improve the testing of their algorithms to make illegal content harder to disseminate.
- **Protecting children from abuse and exploitation online.** Our Codes include important measures to tackle online grooming. These will mean that, by default, children's profiles and locations – as well as friends and connections – will not be visible to other users, and non-connected accounts cannot send them direct messages. Children should also receive information to help them make informed decisions around the risks of sharing personal information, and they should not appear in lists of people users might wish to add to their network. This will make it harder for perpetrators of grooming activity to identify and contact vulnerable children.
- **Our Codes set an expectation that high-risk providers use an automated tool called hash matching to detect Child Sexual Abuse Material (CSAM).** This will help prevent the circulation of this damaging material, disrupting offenders, and flagging to services to report these offences. In response to feedback on our Consultation, we have expanded the scope of our CSAM hash-matching measure to capture smaller file-hosting and file-storage services. These services are at particularly high risk of being used to distribute CSAM.
- **Identifying fraud.** Under the Codes, providers will need to establish a dedicated reporting channel for organisations with fraud expertise. This will help them to identify fraudulent activity quickly.
- **Protecting women and girls.** Women and girls are disproportionately affected by certain online harms. Our measures mean users will be able to block and mute others who are harassing or stalking them. Our Codes will also require providers to take down intimate image abuse (or "revenge porn") material when they become aware of it. Following stakeholder feedback, we have also provided guidance on how providers can identify and remove content posted by organised criminals who are coercing women into prostitution against their will.

- **Guidance to identify illegal content**. On harms which particularly affect women and girls, we have made it easier for platforms to understand how to identify illegal content such as intimate image abuse, sexual exploitation and cyberflashing. In finalising our guidance, we have carefully considered risks to user rights.

Enforcing the rules

From today, providers in scope of the illegal content duties in the Act must act to undertake their Illegal Harms Risk Assessments, which must be completed by 16 March 2025. Our guidance outlines a process that providers can take to understand the harms presented by their service; assess the risk of harms; decide which measures they need to take to manage those risks; implement and record appropriate measures; and report, review and update their risk assessments on a regular basis.

The Government will lay the final Codes in Parliament today. From 17 March, once the Codes have completed the Parliamentary process, providers will need to take the steps laid down in the Codes or use other effective measures to protect users.

Ofcom is already working actively to promote compliance across the industry. Our supervision teams, made up of interdisciplinary experts, have been working over the past year to develop a deep understanding of certain services and to ensure that we have identified the relevant, accountable, senior staff. This proactive engagement has already given us a head start in achieving early, concrete changes next year.

We are also developing support tools to help companies, especially SMEs, to understand and comply with their duties. But we are also well-advanced in preparing for enforcement action and we will not hesitate to take early action against deliberate or flagrant breaches where we believe this to be necessary to prevent serious harm to users. We have the powers to impose penalties of up to £18 million or 10% of the provider's qualifying worldwide revenue (whichever is greater), as well as seeking – in very serious cases –a court order to impose business disruption measures, which may require third parties (such as providers of payment or advertising services, or internet service providers) to withdraw, or limit access to, the services in the UK.

We expect our early enforcement action to focus on ensuring that services are adequately assessing risk and putting in place the measures that will have greatest impact in protecting users, especially children, from serious harms such as those relating to CSAM, fraud, and child access to pornography. Alongside targeted action against specific services, we will also launch broader multi-service or sector-wide compliance programmes once the key safety duties come into force, where we believe there may be systemic issues that need swift and comprehensive action across multiple firms to achieve the necessary change.

What happens next?

In the spring, we will take steps to strengthen the Illegal Harms Codes with an additional consultation. We are currently considering further measures including:

- AI for detecting illegal content including new child sexual exploitation material;
- hash-matching measures for terrorist and intimate image abuse content;
- blocking accounts of those found to have shared CSAM; and
- crisis response protocols for when a crisis emerges.

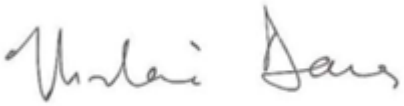
Beyond these Codes, we will continue to bring in other elements of the online safety regime. In January we will publish our final guidance on age assurance, including for publishers of pornographic content, and on children's access risk assessments. In February we will publish our draft guidance

for consultation on protecting women and girls, and in April we will publish our final Codes on the Protection of Children.

I would like to put on record our gratitude for the huge amount of engagement we have had from many stakeholders and Parliamentarians, including but not limited to formal responses to our Illegal Harms consultation. We look forward to continuing to work with you as we build upon these protections in the future.

Today marks the moment when the online safety regime goes live. At Ofcom we will be doing everything we can to ensure that 2025 is a year of action across the industry, with concrete changes made to ensure a safer life online for everyone across the UK.

Yours sincerely,



Melanie Dawes

Technical note: NCII and the Online Safety Act

In her letter of 3 December 2024, the Chair of the Women and Equalities Select Committee asked Ofcom to clarify our position in relation to two topics that have come up during the Committee's inquiry. This technical annex addresses the Committee's questions on these topics in turn.

Ofcom's enforcement powers against non-compliant websites hosting NCII

The Committee asked:

- *Given that it is not possible to submit individual complaints about NCII content being hosted on non-compliant websites to Ofcom, what are the pathways that would lead to Ofcom taking enforcement action against these sites?*
- *How long might engaging in such enforcement action reasonably take?*

For example, how long could it feasibly take before Ofcom could utilise its enforcement powers against a non-compliant website that hosted NCII content? Ofcom officials have previously indicated that they are unable to specify the above because the time taken for enforcement action would be "case-specific", but the Committee would like to know a general timeframe – would such action against a website based in Russia that is dedicated to hosting NCII content, for example, take days, weeks, months or years?

Ofcom has published guidance on our enforcement powers (the "Enforcement Guidance"). It explains the process that Ofcom will usually follow when a potential compliance issue comes to our attention, and the factors Ofcom consider when deciding whether to exercise our enforcement powers under Part 7, Chapter 6 of the Online Safety Act.

Potential compliance issues may come to our attention from a variety of sources, for instance:

- where a service provider proactively informs us about concerns they may have about their own compliance with their obligations;
- where an issue has come to light through Ofcom's regular engagement with a service provider or other relevant third party;
- via our routine monitoring of information provided to our Consumer Contact Team or online safety complaints portal; or via our routine monitoring of information provided to us by service providers;
- where we have concerns about a service provider's response to the exercise by Ofcom of other regulatory functions under the Act;
- a complaint by an industry stakeholder or whistleblower;
- information provided to us by other bodies; or
- a super-complaint submitted by an eligible entity.

When deciding whether to open an investigation or take some other action, the factors we will generally consider include the risk of harm or seriousness of the alleged contravention under consideration, its strategic significance, and the resource implications and risks in taking enforcement action.

Not all issues will lead to an investigation, and in our Enforcement Guidance we also explain the alternative compliance tools that we may use in response to compliance concerns (which include compliance remediation and warning letters as well as enforcement programmes).

The length of time required for an investigation varies depending on the scope and complexity of the investigation and whether the provider disputes the case. However, we must carry out a fair process which, as set out in our Enforcement Guidance, includes an opportunity for the provider concerned to make representations. In urgent cases, we may expedite the process, but typically we would expect an investigation to take some months.

As set out in section 9 of our Enforcement Guidance, Ofcom can apply to the court for business disruption measures if we have sufficient evidence that the relevant statutory tests for making such an application have been met. In most cases, we would expect to gather such evidence as part of a formal enforcement process. However, there may be cases where sufficient evidence has come to light that would prompt us to make an application prior to opening a formal enforcement process. Section 9 of our Enforcement Guidance also gives examples of circumstances where we might consider that a business disruption measure would be appropriate and proportionate. The timetable for such a process would be set by the court. Since these are new powers, we are not yet in a position to estimate likely timings.

Service provider obligations regarding NCII and CSAM (child sexual abuse material)

The Committee asked:

- *Will search engines be required to delist NCII content, as is the case with CSAM?*
- *Will ISPs be encouraged to block access to NCII content hosted overseas, as is the case with CSAM?*
- *What are the differences, if any, in how User-to-User services should treat NCII versus CSAM according to Ofcom's guidance?*

Firstly, it is worth explaining the differences in how the CSAM and NCII offences work. The Online Safety Act identifies CSAM and Intimate Image Abuse as priority offences, however the constituent parts of the respective offences are different. In the case of CSAM, it is illegal to make, show, distribute or possess an indecent image of a child. The content itself is illegal because of the characteristics of the image or video, and in an online context any such content posted, sent or stored is illegal. In the case of NCII, under UK law currently, it is an offence to share or threaten to share (or in Scotland, disclose or threaten to disclose) an intimate image without the consent of the person depicted. NCII content meeting these criteria must be taken down by the service as with CSAM.

Importantly, however, in the case of NCII the service will need to have grounds to infer that the person in the image did not consent to sharing of the image and that the person sharing the image did not have a reasonable belief in consent or that they shared the image with the intention of causing the victim alarm, distress or humiliation. These are additional factors that may not be apparent on the face of the content itself but which must be assessed before an image can be considered NCII and subject to the takedown duty. It is also not currently illegal to create or store intimate images featuring adults without their consent, only to share/disclose such images (or

threaten to do so). We note the government's announcement on 7 January 2025 that they intend to criminalise the making of intimate images without consent, including via Generative AI, in the forthcoming Crime and Policing Bill, which would of course affect the legal position set out above.

Our Illegal Content Judgements Guidance sets out clear guidance for sites and apps to apply when assessing content reported to them. However, these different legal positions create additional challenges in tackling NCII, particularly where technology is used to identify and take down content at scale because it needs to be able to distinguish between consensual and non-consensual content.

User-to-user services

As set out above, the statutory safety duty means that a *user-to-user* service provider must have proportionate systems and processes to take down illegal content, including NCII content, when it becomes aware of it. Our Codes contain recommendations for providers to comply with the safety duty. Our Codes for user-to-user services, which have just been laid before Parliament, do not distinguish between different kinds of illegal content in implementing this duty (see Recommendation ICU C2). As such, once content is identified as CSAM or NCII it is subject to the takedown duty.

In our Codes, Ofcom has also recommended that certain user-to-user services use hash matching technology to detect and remove CSAM content, allowing it to be identified and taken down swiftly (Recommendation ICU C9). Ofcom also recommends that certain user-to-user services use URL matching technology to detect and remove links to locations previously identified as hosting CSAM. In this respect the Codes treat CSAM and NCII content differently for user-to-user services. However, as set out above and in our Statement Overview, we are working towards producing a further Consultation in Spring 2025 on expansions to the Codes, including on the use of hash matching to prevent the sharing of NCII. Ofcom will also include further steps on this in our forthcoming guidance on protecting women and girls online, to be published in February 2025.

Search services

A *search* service provider has a duty to take proportionate steps to minimise the risk of users encountering priority illegal content, including NCII content, in search results. The Codes for search services (see Recommendation ICS C1) say that a search service provider should take appropriate moderation action which results in illegal content no longer appearing in search results presented to United Kingdom users (delisted or deindexed); or being given a lower priority in the overall ranking of search results presented to United Kingdom users (downranked). These Codes are not prescriptive as to whether illegal content should be delisted, deindexed or downranked. In deciding on the appropriate moderation action, Ofcom's Codes say the provider should consider the prevalence of illegal content hosted at the URL or in the database at which the search content concerned is present; the interests of users in receiving any lawful material that would be affected; and the severity of potential harm to United Kingdom users that may arise if they encounter the content, including whether the content is priority illegal content and the potential harm to children. In practical terms, however, we would expect our guidance to mean that a site that is dedicated to NCII or which hosts significant volumes of NCII would be removed from search results.

Ofcom's Codes also recommend that search service take steps to remove URLs identified as hosting CSAM from search results.

ISPs

Ofcom does not regulate ISPs under the Online Safety Act. However, the definition of illegal content means that content all over the world can be illegal content under the Act. This means that user-to-user service providers and search service providers with links to the UK have duties in relation to illegal content hosted overseas, including NCII illegal content.