House of Commons

Women and Equalities Committee

Tackling non-consensual intimate image abuse

Fourth Report of Session 2024–25

HC 336

Women and Equalities Committee

The Women and Equalities Committee is appointed by the House of Commons to examine the expenditure, administration, and policy of the Government Equalities Office and its associated public bodies.

Current membership

Sarah Owen (Labour; Luton North) (Chair)

Alex Brewer (Liberal Democrat; North East Hampshire)

David Burton-Sampson (Labour; Southend West and Leigh)

Rosie Duffield (Independent; Canterbury)

Kirith Entwistle (Labour; Bolton North East)

Natalie Fleet (Labour; Bolsover)

Catherine Fookes (Labour; Monmouthshire)

Christine Jardine (Liberal Democrat; Edinburgh West)

Samantha Niblett (Labour; South Derbyshire)

Shivani Raja (Conservative; Leicester East)

Rachel Taylor (Labour; North Warwickshire and Bedworth)

Powers

The Committee is one of the departmental select committees, the powers of which are set out in House of Commons Standing Orders, principally in SO No. 152. These are available on the internet via www.parliament.uk.

Publication

This Report, together with formal minutes relating to the report, was Ordered by the House of Commons, on 26 February 2025, to be printed. It was published on 5 March 2025 by authority of the House of Commons.

Committee reports are published on the Committee's website at www.parliament.uk/womenandequalities and in print by Order of the House.

Contacts

All correspondence should be addressed to the Clerk of the Women and Equalities Committee, House of Commons, London SW1A 0AA. The telephone number for general enquiries is 020 7219 4452; the Committee's email address is womeqcom@parliament.uk. You can follow the Committee on X (formerly Twitter) using @CommonsWEC, and on Bluesky using @commonswomequ.parliament.uk.

Contents

Summary

Non-consensual intimate image (NCII) abuse occurs when intimate content is produced, published, or reproduced without consent, often online. It is a deeply personal crime that can have life-changing consequences.

While the Online Safety Act (OSA) defines an intimate state as engaging in a sexual act, (partial) nudity or toileting, NCII abuse can also include material that is considered "culturally intimate" for the victim, such as a Muslim woman being pictured without her hijab. The Government should expand the legal definition to include such images.

The OSA creates criminal offences for individuals relating to NCII and places duties on regulated search services and user-to-user services (e.g. social media), including a requirement to take down NCII content. Ofcom also has powers to enforce providers' compliance with the Act, like imposing fines and applying for service restriction orders.

While many platforms remove NCII content voluntarily, some fail to comply with requests to take material down. Around 10% of content remains online, invariably hosted on sites based overseas. The new regulatory regime overseen by Ofcom is unlikely to have much impact on such sites.

Ofcom's current enforcement powers are too slow and not designed to help individuals get NCII on non-compliant websites taken down. In such circumstances, access to those sites should be blocked. For internet infrastructure providers to take this threat seriously and block access to websites that refuse to comply, NCII should be brought in line with child sexual abuse material (CSAM) in law.

The Government should bring forward amendments to the Crime and Policing Bill to make possession of NCII an offence. The Government should also create voluntary guidance for internet infrastructure providers on tackling NCII, like it has for CSAM.

The Government should also take a holistic approach to legislating against NCII abuse by introducing a swift and inexpensive statutory civil process, as has been established in other jurisdictions. This would empower survivors to take fast and effective action towards having NCII taken down or blocked. Such a regime should be alongside and underpin the creation of a registry of NCII content that internet infrastructure providers are requested to prevent access to, similar to the current arrangements for CSAM.

The statutory regime should enable civil courts to make orders, including designating an image as NCII content and ordering its inclusion on the aforementioned registry, as well as requiring an individual to delete any such images.

The Government should also set up an Online Safety Commission, similar to the eSafety Commission in Australia, with a focus on support for individuals. The new Commission would be able to apply for and send such court orders and oversee the aforementioned NCII registry.

Survivors are being re-traumatised by police when reporting NCII abuse. The Revenge Porn Helpline (RPH) told us that victims had been asked not to take down their NCII so that it would remain online during their court case. The College of Policing, Ofcom, and the RPH together should produce guidance to improve the police response to reports of NCII abuse.

There have been cases where, following the criminal justice process, perpetrators have had devices containing the NCII returned to them; this is harrowing for victims. The Government, Sentencing Council and Crown Prosecution Service must each take steps to ensure that those charged with NCII offences are deprived of that material.

An online crime like NCII abuse can be just as damaging as physical violence. The Criminal Injuries Compensation Scheme was established to provide compensation to those physically or mentally injured from a violent crime. Its eligibility criteria must be amended to ensure NCII is clearly within its scope.

The RPH launched a free 'hashing' tool designed to protect people from NCII abuse. Hashing generates a digital fingerprint that uniquely identifies an image or video. This is distributed to participating platforms to allow them to prevent that content being uploaded. Disappointingly, some major platforms, including Google, have so far not joined the 13 currently participating platforms; they should do so urgently. We welcome Ofcom's plans to launch a consultation on expansions to its Codes of Practice that would include proposals on the use of hashing; our view is clear, these proposals should include requiring companies to utilise the technology.

Synthetic NCII, known also as 'deepfakes', refers to any sexual or nude media created using AI that represents the likeness of another individual without their consent. The Government's plans to criminalise their creation are welcome. However, the offence must be based on the lack of consent of the victim, not motivation of the perpetrator. The creation and use of nudification apps should also be criminalised.

The consequences of NCII abuse can be life-changing and tragic. The OSA represents considerable progress in this area, as do the additional offences included in the Crime and Policing Bill and Data (Use and Access) Bill, but significant gaps in the legislative and regulatory framework remain. The Government must take the further steps we have outlined in this report to ensure that it does not miss the opportunity to do all it can to protect adults from this rapidly growing harm.

1 Introduction

1. Non-consensual intimate image (NCII) abuse occurs when intimate content is produced, published, or reproduced without consent, often online. It is a deeply personal crime which can have life-changing and life-threatening consequences. It takes great courage for someone to report being a victim to it, particularly to the police.

What is NCII?

2. Non-consensual intimate content can be produced consensually or non-consensually. Consensually produced content is content that the victim themself has created, often in scenarios of fear or pressure. In these circumstances perpetrators may coerce their victims into sharing the intimate content either through grooming—the building of trust with a victim in order to exploit them—or sextortion, where a victim is blackmailed under the threat of intimate content being shared.[1] Consensually produced content also includes content that is stolen via the hacking of an individual's private data.

3. Non-consensually produced content includes content that is captured without the victim's knowledge, where the perpetrator themselves takes the non-consensual intimate images or videos "either during a sexual encounter or even in a public setting such as a public restroom, public pool or locker room".[2] While the Online Safety Act describes an intimate state as engaging in a sexual act, (partial) nudity or toileting,[3] NCII abuse can also include material that is culturally embarrassing for the victim. The Law Commission identified broadly two types of such image: those that identify someone as LGBTQ+ when their family, friends, or community may not know or accept them as such, and those that are considered intimate by particular religious groups.[4]

---

1 Grooming refers to "intentionally building a relationship with a minor to lower their inhibitions and prepare for sexual activities. This behaviour is calculated and is usually for sexual or financial purposes. Once trust is established the groomer starts to desensitise the child to sexual content and use secrecy, and shame". Sexual extortion, also called 'sextortion', is "a type of blackmail. The perpetrator demands sexual favours, money, or other benefits under the threat of sharing intimate or sexually explicit material". See InHope, 'What is NCII?', accessed 1 May 2024

2 InHope, 'What is NCII?', accessed 1 May 2024

3 Online Safety Act 2023, s.66D(5)

4 Law Commission, Intimate image abuse: a final report, 6 July 2022, p 82

4. Whilst NCII is often referred to as "revenge porn", we have chosen not to use this term, since revenge is not the only possible motivation for this abuse. Furthermore, the term implies that the victim has done something to deserve what has happened.

The scale of the problem

5. Research has shown that 1 in 14 adults in England and Wales—including 1 in 7 women and 1 in 9 men aged 18–34—have had or have experienced threats to have their intimate or sexual images shared.[5] Since 2015, the Revenge Porn Helpline,[6] which is run by the charity South West Grid for Learning (SWGfL) to assist adults in the UK to get their content taken down, has reported approximately 338,000 intimate images to platforms for removal, 306,000 of which have been successfully removed from the internet.[7] The Helpline has seen a surge in demand. David Wright CBE, Chief Executive of SWGf, told our predecessor Committee:

> in 2019 we managed 1,600 cases; that doubled in 2020, we think fuelled by covid, to 3,200, then to 4,400 in 2021, 8,900 in 2022 and then last year—we only published this data yesterday—it was just under 19,000 cases. So, we have seen a tenfold increase in four years.[8]

Figures for 2024 show the caseload increasing further, with the Helpline having received 22,276 cases. These figures only include those reporting to the Helpline, there are many more individuals who do not.

6. Some of the cases the Revenge Porn Helpline deals with are astounding in scale. We were told of a case with a single perpetrator but approximately 2,000 victims internationally; in one trade, the perpetrator sold a terabyte of content to a buyer that amounted to 1,000 hours of video and 310,000 photographs.

7. NCII is a deeply gendered threat. In 2023, 71% of reports received by the Revenge Porn Helpline were made by women (where the client's gender was known). In cases where the gender of the perpetrator was known, over 81% were male, with 67% of the offenders being a current or former partner. On average, women experienced over 28 times more images being shared

5 Refuge, The Naked Threat, 6 July 2020

6 The Revenge Porn Helpline was established in 2015 following the criminalisation of the sharing of intimate images without consent under the Criminal Justice and Courts Act 2015. The Helpline assists adults in the UK that have been affected by intimate image abuse with getting their content taken down by reporting it to platforms and websites for removal. It also provides practical advice and information on the law around NCII abuse and how to report it to the police.

7 Revenge Porn Helpline, 'Revenge Porn Helpline 2023 Report' (7 May 2024), p 5

8 Oral evidence taken on 8 May 2024, Q51

than men. However, in sextortion cases, nearly 93% of cases involved male victims, with the perpetrators consisting predominantly of organised criminal gangs, potentially based abroad.[9]

The inquiry

8. This inquiry was begun by our predecessor Committee in May 2024. That Committee met with multiple victims of NCII abuse, including campaigner and broadcaster Georgia Harrison who gave formal evidence to the Committee.[10] It also invited written evidence, including from survivors of NCII abuse. They chose not to publish the majority of submissions in order to protect the identities of the contributors. We have taken a similar approach. As well as taking further evidence, we have also had private briefings from experts in this crime from both within the UK and in other jurisdictions.

9. We are immensely grateful to everyone who has assisted us in this work, but particularly those who have shared their experiences of NCII abuse. We understand the challenges involved in sharing details of this abhorrent crime with a parliamentary committee. The strength and bravery contributors have shown in doing so is admirable, and we thank them for giving us such valuable insight. We would also like to thank Professor Clare McGlynn and Professor Lorna Woods for sharing their expertise with the Committee.

9 Revenge Porn Helpline, 'Revenge Porn Helpline 2023 Report' (7 May 2024), p 12
10 Oral evidence taken on 8 May 2024, Q1–28

2 The impact of abuse

10. Victims of NCII abuse have described the far-reaching and continuing impact the abuse has had on their lives, their confidence and their relationships. TV personality and campaigner Georgia Harrison told our predecessor Committee what happened in her case:

> in 2020 an ex-partner of mine filmed us having sex without me knowing. […] I was then assured on that day that it would go no further than those four walls, that the footage would be deleted […] Six months down the line I was then sent a screenshot of the footage in question from a fan […] located in America, so as soon as I saw that image I immediately knew that somehow the footage that I had been told would never ever go anywhere had been spread globally online. I just was not aware of how or where it had come from, so obviously I then immediately asked this fan, "Where have you seen this?" I was then told it was on the person in question's verified OnlyFans account.[11]

Georgia took the perpetrator to court and secured a prosecution against him.[12] Speaking about her own experience of NCII abuse, she explained:

> It impacted me in every way you could imagine. So I always sort of compare it to grief: you have to actually grieve a former version of yourself, you feel like you lose your dignity and a lot of pride, there is so much shame involved in it. For the first few days I was really just going through waves of complete sorrow and shock.[13]
>
> […] It got to the point where I was so emotionally affected by what happened to me that I ended up being physically ill as well, to the point where I was in hospital […] the stress took such an effect on my body that I ended up having a cyst burst and I got an infection. It was literally just like my body deteriorated with my emotions.[14]

11. Georgia Harrison is not alone in her experiences. One contributor to our inquiry described the impact of their NCII remaining online as "exhausting":

11 Oral evidence taken on 8 May 2024, Q1
12 ITV News, Georgia Harrison speaks up for 'all the victims' after ex Stephen Bear jailed over sex tape, 3 March 2023
13 Oral evidence taken on 8 May 2024, Q11
14 Oral evidence taken on 8 May 2024, Q11

> I am terrified of applying for jobs for fear that the prospective employer will google my name and see. I am terrified when meeting new people that they will google my name and see. I am terrified that every person I meet has seen. I am terrified of having social media accounts and have deleted all of them in case the people who continue re-posting my images will be able to contact me. In fact, before I deleted my social media, I received endless messages from strangers who had viewed my images and were trying to contact me. It was terrifying. I have been minding my own business on a night out and had someone tell me they have seen my images. I have been at work and had a stranger come and tell me they have seen my images. It simply never stops.[15]

12. Contributors to our inquiry explained how they had "drastically altered" their life plans and aspirations in order to live a life in obscurity, in one case legally changing their name to escape the online fallout, because their full name had been published alongside their non-consensual content.[16] One survivor observed that, as horrific as it sounded, they sometimes wished that they had been subjected to a physical sexual assault rather than an online one, so that at least the replaying of the abuse would be within the privacy of their own head, rather than online for anyone to see.[17]

Revenge Porn Helpline

13. The Revenge Porn Helpline organisation supports survivors of NCII abuse in getting their content removed and can help prevent it being reuploaded. They are effective at removing NCII content reported to them, with a takedown rate of over 90%.[18] But getting content taken down is reliant on the platforms it is hosted on being compliant, which is not always the case. Indeed, we were told of people whose content is still circulating more than seven years after their perpetrator shared it, with the Revenge Porn Helpline still having to make monthly reports to platforms to get it removed.[19]

14. The immediate priority for victims of NCII abuse is the urgent take down of their content. David Wright CBE, told our predecessor Committee:

> When the team are supporting victims, I am continually reminded that when they want help and support, they want help and support now. They want their content removed now, not in a few hours or a few days.[20]

15 Evidence submitted in confidence
16 Evidence submitted in confidence
17 Evidence submitted in confidence
18 Q15
19 Evidence submitted in confidence
20 Q32

Georgia Harrison used her experience to explain why time matters:

> it is really like a house fire, the quicker you can put it out the quicker you can stop it. Unfortunately in four to six days your house has burnt down and it is just too late, everyone knows about this video: your family, your workplace, your peers. However, if you can get through to someone in the first 24 hours, you then have time to stop this going any further and potentially not ruining your life. But for me it went as far as you can imagine, to the point where it was global.[21]

15. The Revenge Porn Helpline provides essential support by removing the heavy burden on survivors of NCII abuse to navigate the content removal and justice processes as well as providing vital emotional support.[22] Georgia Harrison described her experience with them:

> Not only can they give you support in terms of therapy and advice, but they can try to track this imagery down and get it back before your employer or your family find out about it. But the only help for these victims right now is the RP Helpline; it is literally all there is, and it is not a big team.[23]

16. Services such as the Revenge Porn Helpline require long term and needs-based funding to enable them to meet accelerating demand on their services, allow them to invest in necessary technical development for an evolving online environment and adapt the support they provide in response to emerging forms of violence against women and girls (VAWG).[24] Yet, we heard that their Home Office funding remains at 2020 levels, making it a challenge for them to keep up with demand and preventing them from developing online tools that could streamline reporting and removal processes.

17. **RECOMMENDATION**

The services provided by the Revenge Porn Helpline need to be supported by sufficient funding to allow them to keep up with demand and ensure that no victim of NCII goes unsupported. Current Government funding has remained at 2020 levels despite a sevenfold increase in caseload. Future funding must increase and should be multiyear to provide a sustainable footing and allow the development of the tools necessary to help its services keep pace with the increased volume and technical sophistication of NCII abuse in the UK.

21 Oral evidence taken on 8 May 2024, Q1

22 End Violence Against Women Coalition #NotYourPorn, Glamour UK, Professor Clare McGlynn, Stop Image-Based Abuse, September 2024

23 Oral evidence taken on 8 May 2024, Q27

24 End Violence Against Women Coalition #NotYourPorn, Glamour UK, Professor Clare McGlynn, Stop Image-Based Abuse, September 2024

Victim experience of the Criminal Injuries Compensation Authority

18. The Criminal Injuries Compensation Authority (CICA) was established to provide injury awards and other compensatory payments to "people who have been physically or mentally injured because they were the victim of a violent crime in England, Scotland or Wales".[25] The Criminal Injuries Compensation Scheme (CICS) sets out what constitutes a crime of violence for the purposes of being eligible for compensation.

19. We and our predecessors spoke to victims of NCII abuse who told us that they had been advised to apply to the Scheme to get support with the costs of their ongoing counselling. However, they were told that their applications were refused because acts such as online sexual abuse do not currently constitute a crime of violence for the purposes of the Scheme unless the act caused 'fear of immediate violence'.

20. When the Minister was asked during our oral evidence session if she would commit to making online abuse eligible under the scheme, she replied:

> The point about CICA is not true. I am aware of victims and survivors who have had redress through the scheme […] One of the awards can be made as the result of disabling mental injury […] But I am aware of victims and survivors who are eligible to claim compensation. If victims and survivors do not know that, we need to make them aware of the victims code, which explicitly sets out what they are eligible for. We need increased awareness of it so that they can claim[26]

21. We asked CICA to clarify the circumstances under which victims of NCII abuse may be eligible for compensation under the scheme. They replied:

> A victim of NCII abuse may be eligible for compensation if the incident meets the definition of a "crime of violence" […] and they have sustained a "disabling mental injury" […] a "crime of violence" includes "a threat against a person, causing fear of immediate violence in circumstances which would cause a person of reasonable firmness to be put in such fear".
>
> Offences committed from a distance, like NCII abuse, will be considered a "crime of violence" if they fall within this definition. A "disabling mental injury" is a mental injury with a substantial adverse effect on someone's ability to carry out normal day-to-day activities.[27]

25 Gov.uk, 'Criminal Injuries Compensation Authority', accessed 22 May

26 Q124

27 Correspondence with the Criminal Injuries Compensation Authority, 11 December 2025

22. It is difficult to see how the criteria above could apply in all but the rarest cases of NCII. Although some victims of NCII may fear violence and feel threatened (particularly where their personal details have been shared), whether this could be interpreted to be a "fear of immediate violence" is unclear. It is evident that the criteria were not written with the world of online violence in mind and do not recognise the real harms that it causes. None of the survivors we spoke to, who had endured truly awful experiences, had been successful in their applications to the Scheme.

23. We asked CICA how many victims of NCII abuse have successfully claimed compensation under the CICS in the last five years. They told us they were unable to provide figures, since "awards of compensation are made in respect of the physical and/or mental injuries sustained by the victim rather than the type of offence committed".[28]

24. The Ministry of Justice (MoJ), which has policy responsibility for CICA, consulted on the Scheme in 2020, 2022 and most recently in summer 2023 in response to the final report of the Independent Inquiry into Child Sexual Abuse, which recommended that the scope be extended to include forms of child sexual abuse such as online-facilitated sexual abuse.[29] The MoJ is currently considering the responses to those consultations as part of a comprehensive review of the Scheme. A decision on whether to amend the scope of the Scheme has yet to be announced.[30]

25.

CONCLUSION

The list of offences that are within scope of the Criminal Injuries Compensation Scheme is out of date. Crimes perpetrated online, such as non-consensual intimate image abuse, can be just as damaging to a person as those involving physical violence. They can have a catastrophic impact on a person's mental health. It is essential that victims of such crimes are able to access compensation.

26.

RECOMMENDATION

The Ministry of Justice must amend the eligibility criteria of the Criminal Injuries Compensation Scheme to bring claims from victims of sexual offences perpetrated online, specifically non-consensual intimate image abuse, within its scope.

28 Correspondence with the Criminal Injuries Compensation Authority, 11 December 2025

29 Independent Inquiry: Child Sexual Abuse, The Report of the Independent Inquiry into Child Sexual Abuse, October 2022 pg 291

30 Gov.uk, Criminal Injuries Compensation Scheme Review: additional consultation 2023, accessed 12 Feb 2025

3 The legal and regulatory framework

Online Safety Act 2023

27. The Online Safety Act (OSA) aims to protect children and adults online. It broadly takes a two-pronged approach to tackling NCII: first, it creates criminal offences for individuals relating to NCII; and second, it places general duties on regulated search services and user-to-user services (e.g. social media), making them more responsible for their users' safety, to reduce risks that their services are used for illegal activity, and to remove illegal content when it does appear.[31]

28. The Act requires Ofcom to develop guidance and codes of practice that set out how online platforms can meet their duties. Ofcom is carrying out public consultations on draft codes of practice before finalising them.[32] Services can be in scope of the OSA even if the provider of the service is based outside the UK, for example, where it has links with the UK, including a significant number of UK users, or if the UK is a target market.[33]

New sharing intimate image offences

29. OSA imposes criminal liability on individuals for certain activities relating to NCII. Section 188 OSA created four new criminal offences relating to intimate image abuse by amending the Sexual Offences Act 2003 ('SOA 2003') and inserting a new s.66(B) into that Act. Section 66B(1) creates a new 'base' offence of sharing intimate images without consent. Section 66B(2) creates an offence of sharing intimate images without consent with the intention of causing a person alarm, distress or humiliation, while s.66B(3) creates an offence of sharing intimate images without consent or reasonable belief in

31 Gov.uk, Online Safety Act: explainer, published 8 May 24; Correspondence from Parliamentary Under-Secretary of State, Ministry of Justice & Parliamentary Under-Secretary of State Home Office: Tackling non-consensual intimate image abuse, 20 Dec 2024

32 Gov.uk, Online Safety Act: explainer, published 8 May '24

33 Correspondence from Parliamentary Under-Secretary of State, Ministry of Justice & Parliamentary Under-Secretary of State Home Office: Tackling non-consensual intimate image abuse, 20 Dec 2024

consent for the purpose of a person obtaining sexual gratification.[34] Section 66B(4) makes it an offence for a person to threaten to share intimate images with the intention that the person being threatened or another person who knows them will "fear that the threat will be carried out", or if they are reckless as to whether the person being threatened or someone who knows the person being threatened will fear that the threat will be carried out.[35] The Act also makes it clear that the prosecution does not need to prove "that the photograph or film mentioned in the threat exists".[36]

30. Section 190 OSA repealed the previous offence under section 33 of the Criminal Justice and Courts Act 2015, as well as related criteria under sections 34 and 35. The section 33 offence had required victims to prove that their perpetrator had disclosed (or threatened to disclose) private sexual photographs and films with the *intent* to cause distress.[37] The new base offence removes the need to prove a motivation to cause distress, something that campaigners including Georgia Harrison have been calling for.[38]

The duties on regulated services

31. OSA places a number of duties on user-to-user services and search services which are regulated under the Act. As part of this, OSA introduced "a new legal concept" of 'illegal content'.[39] Content will constitute 'illegal content' for the purposes of the Act if the use, possession, viewing, accessing or publication of such content amounts to a 'relevant offence'.[40] There are two types of 'relevant offence' under OSA: first, 'priority offences', which include the most serious offences such as terrorism offences and child sexual abuse offences;[41] second, other relevant offences, which broadly includes most other criminal offences against an individual.[42]

32. There are additional duties on regulated services regarding priority illegal content, i.e. content involved in a priority offence.[43] In particular, OSA requires regulated user-to-user services to have proportionate systems

34 Sexual Offences Act 2003, section 66B(2) and (3) (inserted by the Online Safety Act 2023, section 188); Correspondence from the Minister for Victims and Violence Against Women and Girls, dated 6 Jan 2025

35 Sexual Offences Act 2003, section 66B(4) (inserted by the Online Safety Act 2023, section 188);

36 Sexual Offences Act 2003, section 66B(7) (inserted by the Online Safety Act 2023, section 188)

37 Online Safety Act 2023, section 190

38 Gov.uk, 'Government crackdown on image-based abuse', accessed 22 May 2024

39 Online Safety Act 2003, section 59

40 Online Safety Act 2003, section 59

41 Online Safety Act 2003, section 59 and Schedules 5, 6 and 7

42 Online Safety Act 2003, section 59

43 Online Safety Act 2003, section 59

and processes in place to minimise the length of time for which any priority illegal content is present on their services and, when alerted by a person to the presence of such content, to swiftly take it down.[44] It also requires providers to take proportionate steps to prevent or minimise users encountering priority illegal content.[45]

33. There is therefore a key difference between whether content is priority illegal content or just illegal content under OSA: regulated services are only required to have systems to remove illegal content relating to non-priority criminal offences once they are aware of it, but do not have a duty to prevent users encountering it.[46] Ofcom's Codes of Practice set out recommended measures for how providers can meet their obligations in relation to both illegal content and priority illegal content. Subject to the Codes of Practice completing Parliamentary process, from 17 March 2025, providers will need to take the safety measures set out in the Codes of Practice or use other effective measures to protect users from illegal content and activity.[47]

34. In September 2024, the Government announced it would amend OSA to make sharing intimate images without consent a 'priority offence', which the Government described as "putting them on the same footing as public order offences and the sale of weapons and drugs online".[48] The sharing offences were added into Schedule 7 of the OSA via statutory instrument in November 2024, and will come into effect alongside illegal content duties (see below).

35. When making judgements about content, the OSA requires service providers to do so based on all relevant information that is reasonably available to them.[49] The approach is to consider—based on this reasonably-available information—whether there are reasonable grounds to infer that all elements necessary for the commission of an offence, including the mental elements, are present and satisfied, and that there are no reasonable grounds to infer that a defence to the offence may be successfully relied upon.[50] Content moderation systems and processes should be set up to take 'illegal content' down at least at the point this threshold is met.

---

44 Online Safety Act 2003, section 10(3)
45 Online Safety Act 2003, sections 10 and 27
46 Gov.uk, Online Safety Act: explainer, published 8 May '24
47 Ofcom, Quick guide to illegal content codes of practice, accessed 14 February 2025
48 Gov.uk, 'Crackdown on intimate image abuse as government strengthens online safety laws', accessed 14 Feb 2025
49 Online Safety Act 2003, sections 192
50 Online Safety Act 2003, sections 192

Removal of illegal content that has been shared, forwarded, or reposted

36. One problem facing survivors of NCII abuse is that their content can continue to spread online, often for years after the original post was removed. Ofcom's draft guidance for platforms initially stated that each time a piece of non-consensual content "has been shared, forwarded or reposted, by a new user, a service should treat it as a new piece of content for the purpose of an illegal content judgement".[51] This meant that platforms were not required to undertake a blanket removal of every instance of the reported image, but to make a judgement on each individual posting/sharing of the image. Not only would this have placed a lot of the responsibility on individuals to seek out each instance of their images being posted and report them, but it would have also created delay in getting them taken down.[52]

37. We are pleased to see that Ofcom addressed this in their updated guidance, as part of their recent statement on illegal harms, which now states:

> we think it is reasonable to infer that absent any evidence that the user reposting, forwarding or resharing content has taken appropriate steps to ascertain consent, they do not have a reasonable belief in consent. It follows that if the content concerned is an intimate image which has been shared without consent, it will be illegal content when it is forwarded, shared or reposted. Our final Guidance reflects this position.[53]

Taking illegal images

38. In January 2025, the Government wrote to us stating that it would introduce new offences for the taking of intimate images without consent and the installation of equipment with intent to enable the taking of intimate images without consent. The new offences were included in the Crime and Policing Bill. To do this, two previously existing voyeurism offences—of recording a person doing a private act, and recording an image beneath a person's clothing (the so-called 'upskirting' offence) in sections 67(3) and 67A(2) of the Sexual Offences Act 2003 respectively—were repealed and replaced with three new offences:

51 Ofcom, Protecting people from illegal harms online Volume 3: Transparency, trust and other guidance, 16 Dec 2024, p59 2.270

52 Professor Clare McGlynn and Professor Lorna Woods [IIA003] para 28

53 Ofcom, Protecting people from illegal harms online Volume 3: Transparency, trust and other guidance, 16 Dec 2024, p59 2.274

i) A "base" offence of intentionally taking an intimate image without consent and without reasonable belief in consent;

ii) An offence of intentionally taking an intimate image without consent and with the intention of causing the victim humiliation, alarm or distress; and

iii) An offence of intentionally taking an intimate image without consent and without reasonable belief in consent, for the purpose of the perpetrator or another person obtaining sexual gratification.[54]

The Government explained:

> "These new offences cover a broader range of behaviours than current offences, providing greater protection for victims."[55]

39. We note that an offence of taking NCII was proposed by Baroness Owen of Alderley Edge in her Non-Consensual Sexually Explicit Images and Videos (Offences) Bill introduced in September 2024.[56] In that Bill, the Baroness defined taking by including the words "otherwise capturing", in order to future proof the law and ensure processes such as screen-shotting are within scope.

40. The Crime and Policing Bill includes a broad definition of content, including that which is a copy, digitally altered or altered 'in any other way' and "data stored by any means which is capable of conversion into a photograph, film or image".[57]

41. **CONCLUSION**
We welcome the inclusion in the Crime and Policing Bill of the new offences of taking an intimate image without consent and of installing equipment for the purposes of enabling the commission of those offences. We also welcome the Government's recognition that the definition of what constitutes an image for these purposes should be broad in scope - something campaigners had been calling for. These measures represent significant legislative progress in the battle to protect people from NCII abuse and punish those who commit it.

54 Correspondence from Minister, Safeguarding and Violence Against Women and Girls and Minister for Victims and Violence Against Women and Girls, re Crime and Policing Bill, dated 25 Feb 2025

55 Correspondence from Minister of State of Justice, re Tackling non-consensual intimate image abuse, dated 22 January 2025

56 Non-Consensual Sexually Explicit Images and Videos (Offences) Bill 2024, clause 1

57 Crime and Policing Bill 2025, clause 66AC ss.5(4B)

Non-compliant platforms

42. Evidence to our inquiry raised concerns that making sharing intimate images without consent a 'priority offence' under the OSA, while helpful, does not go far enough to tackle the problem of non-compliant platforms. Many platforms already remove NCII voluntarily—for example if they breach the platform's terms of service or following reports from victims, the Revenge Porn Helpline, or other advocates. However, some fail to comply with requests to take material down, most commonly those that are based overseas. We heard from the Revenge Porn Helpline that they have around a 90% take down rate—better than many regulators—and that the location of the host is a primary reason for the other 10% remaining online. David Wright CBE, Chief Executive of SWGfL (which runs the Revenge Porn Helpline), told our predecessors:

> We found 200 victims of this one perpetrator, and we reported over 160,000 images that he had extorted of these women. We had 147,000 removed. There [are] a residual 15,000 images online that we are unable to take down.

David Wright further explained:

> There are 30,000 images online that we know are NCII, 15,000 of which—including Georgia's content—remain online, typically in countries where they have no interest [in complying]. They may be hosting this content specifically to generate traffic from different countries, typically Russia or Latin America, where we have no control and they are not going to respond to us. Other regulators around the world only have a 90% take-down rate too. We cannot expect 100% of platforms to remove content. We need other mechanisms to be able to block access to this content to stop the re-victimisation that Georgia powerfully talked about.[58]

Sophie Mortimer, manager of the Revenge Porn Helpline, said:

> we report to over 1,000 different platforms. Much of this content that continues to circulate is on platforms beyond our reach, whose business model is entirely constructed around the sharing and resharing of this content. They have no interest in engaging with us because they do not have to and, sadly, they are also beyond the reach of Ofcom or any other authority to take action. The content is still there, and all it takes is a very small number of images to still be there and recirculate and then you are back to square one.[59]

58 Oral evidence taken on 8 May 2024, Q46

59 Q16

Witnesses told us that it is unlikely that the OSA and new regulatory regime overseen by Ofcom will have much impact on such sites.[60]

Ofcom's powers

43. Ofcom has a broad range of powers to assess and enforce providers' compliance with the Act, including imposing fines that could reach up to 10% of qualifying worldwide revenue. Websites hosted overseas are within scope of these powers. However, David Wright observed:

> Yes, Ofcom will have more powers, so they will have service restriction orders that they can impose to do with payment gateways. If those fail, they will be able to serve service restriction orders to block access to content. I would suggest this is wholly inadequate. We have already heard a lot can happen in 24 hours, but this is going to be months. That is how content can stay online.[61]

44. We asked Alex Davies-Jones, the Parliamentary Under-Secretary of State at the MoJ, what she would advise someone whose NCII was being hosted on a non-compliant website to do. She replied:

> If it is on a non-compliant website, sadly, it is horrendous. I would ask them to seek out victim support and go to somebody to get that support. The problem we have is that until the Online Safety Act is implemented, there is no way of getting that material taken down.[62]

45. Yet, like David Wright, Professors of Law Clare McGlynn and Lorna Woods described Ofcom's powers under the OSA as "not designed to provide individuals with redress";[63] Professor McGlynn described them as being "wholly inadequate for this purpose".[64] Their evidence described the OSA as being "designed to incentivise service providers into designing and running their services better, including by providing better complaints mechanisms".[65] Although Ofcom does have an online complaints portal, the accompanying information makes clear that "Ofcom is not able to respond to or adjudicate on individual complaints".[66]

60 Oral evidence taken on 8 May 2024, Q46; Q16; Q87 [Professor Clare McGlynn]
61 Oral evidence taken on 8 May 2024, Q46
62 Q128
63 Professor Clare McGlynn and Professor Lorna Woods [IIA003] para 1
64 Professor Clare McGlynn [IIA0005] pg3 para 40
65 Professor Clare McGlynn and Professor Lorna Woods [IIA003] para 11
66 Ofcom, Complain to Ofcom, (accessed 10 Feb 2025)

46. The powers of Ofcom to act against non-compliant websites that host NCII are lengthy and bureaucratic. This is especially clear when compared to both the urgency with which NCII content must be removed to mitigate the harm to victims, and the need for thousands of images to be removed across many websites. Professors McGlynn and Woods explained:

> The starting point is an enforcement notice, according to which a provider can be directed to remedy a defect in its systems. Although Ofcom has no powers to make determinations in relation to specific items of content, Ofcom might identify that a service provider dealt with a category of content, such as non-consensual intimate imagery, in an ineffective way.
>
> Again, the enforcement here would be in relation to categories of content, not specific items of content. The service provider may comply with Ofcom's requirements. But this would be in relation to their systems and processes for dealing with categories of content, not specific items of content (albeit that it might have an indirect effect in the service provider removing the items of concern).
>
> Failure to comply leads to fines and ultimately business disruption measures which include 'access restriction orders'. Access restriction orders could be made against an ISP [Internet Service Provider] seeking that it block access to certain sites – section 146 [of the OSA]. However, it should be noted that the process of gaining business disruptions orders is complicated—requiring a court order—and must fulfil specified grounds. They are envisaged as applying at the end of a long enforcement process once other mechanisms have been tried.[67]

47. The Professors' written evidence also pointed out that such measures are "only designed to be used in exceptional circumstances evidenced by the fact that if a business disruption order is granted, the Secretary of State has to be informed", making them "wholly inadequate" to deal with NCII hosted on non-compliant websites.[68] When we asked Ofcom how long engaging in enforcement action would reasonably take, they said:

> In urgent cases, we may expedite the process, but typically we would expect an investigation to take some months.[69]

67 Professor Clare McGlynn and Professor Lorna Woods [IIA003] para 12–14
68 Professor Clare McGlynn and Professor Lorna Woods [IIA003] para 15–16
69 Correspondence with Chief Executive, Ofcom re Tackling non-consensual intimate image abuse, dated 17 Jan 2025 - technical note, pg 2

48. **CONCLUSION**
Ofcom's current enforcement powers, while welcome, are far too slow and not designed to help individual victims get abusive images of themselves on non-compliant websites taken down or have access to them restricted. The duties under the regulatory regime created by the Online Safety Act are a good start. However, further steps are required to effectively tackle the threat posed by NCII at an individual level, particularly where content is hosted overseas.

Potential remedies

Guidance for internet infrastructure providers and a central repository of illegal NCII

49. One way to address the problem of the 10% of sites that do not comply with requests to take down content is to block access to them from the UK, or otherwise disrupt their business model.

50. The Government has published guidance on how internet infrastructure providers (IIPs)—including web-hosting providers, Content Distribution Network (CDN) providers, registries, registrars, anonymising services, Internet Service Providers (ISPs), Mobile Network Operators (MNOs), browsers and app stores—can support efforts to effectively tackle illegal harms such as child sexual abuse and terrorism online.[70] The guidance is separate but complementary to the Online Safety Act. No such guidance exists for NCII, reflecting the current difference between how child sexual abuse material (CSAM) and NCII is treated. David Wright described what the impact of the difference in approach between CSAM and NCII meant at a practical level, after having no success with asking websites to remove material:

> We approached [ISPs] to see if we could block access, as we routinely do with other illegal content. The response was, "No… We are not allowed to be blocking access to legal content".[71]

51. The guidance on CSAM sets out technical steps that companies can take to restrict access to the respective material. These include making use of a URL block list to prevent users accessing CSAM, for example, as provided by the Internet Watch Foundation (IWF) to their members. The IWF describe

70 Home Office, Voluntary guidance for internet infrastructure providers on tackling online child sexual exploitation and abuse, gov.uk, (accessed 10 February 2025); Home Office, Voluntary guidance for internet infrastructure providers on preventing terrorism online, gov.uk, (accessed 16 February 2025);

71 Oral evidence taken on 8 May 2024, Q46

this as a "a dynamic URL list", which provides a comprehensive list of webpages where they have confirmed images and videos of child sexual abuse. IWF Members can use the list, under licence, to block access to criminal webpages. Through the use of their "domain alerts", the IWF are able to alert registry operators so that they can prevent their top-level domains (TLD's, e.g. .uk, .com) from being used to host CSAM.[72] The TLD is then able to take immediate action to suspend the domain or contact the owner. While access to the images and videos is blocked, the IWF works to have the actual picture or video removed from the internet. If an entire website is dedicated to CSAM then the IWF will seek to block it at the domain level, whilst efforts are made to deregister the website. Internet encryption is making blocking at URL level more challenging, but we heard that there remains utility in having such a registry.[73]

52. For a block list or registry of NCII to be created, a determination of non-consent would first be required. CSAM is more straightforward to deal with, in so far as the primary determination is whether the content involves someone under the age of 18, which in most cases can be done by using the image alone. NCII, however, requires a determination of non-consent, which is not feasible using only the image.[74] A possible solution to the issue of identifying material as NCII may involve having a similar expert body to the IWF, but with the additional step of a determination on consent by a civil court (see para 66 below).

53. Differences between how CSAM and other content that is illegal (for the purposes of OSA) is treated can also be seen in Ofcom's Illegal Content Codes of Practice.[75] For example, subject to the Codes completing the Parliamentary process, search engines are encouraged to ensure that CSAM URLs are deindexed based on a list produced by an expert body that is regularly updated.[76] We understand the Internet Watch Foundation (IWF) to be an example of such a body. Furthermore, the draft Code of Practice sets out detailed criteria for ensuring that the body identifying the CSAM is authorised to do so, and the lists and information is kept up to date.[77]

54. The difference in treatment between CSAM and NCII reflects their standing in law. The Protection of Children Act 1978 describes the following as illegal activity:

- To take or make any indecent images of a child (creation)
- To show or distribute such images (sharing)

72 Internet Watch Foundation, Domain Alerts, accessed 10 February 2025
73 Q62
74 Professor Clare McGlynn [IIA0005] pg 4 para 47
75 Professor Clare McGlynn [IIA0005] pg2 para 23
76 Ofcom, Illegal content Codes of Practice for search services, 16 Dec 2024, pg 20
77 Ofcom, Illegal content Codes of Practice for search services, 16 Dec 2024, pg 20

- To possess such images with intent to show or distribute them (possession + intent to share)
- To advertise for showing or distributing such (pseudo-)photographs (advertisement)

55. Although the acts of creation and possession of CSAM have been criminalized, this is not the case for NCII.[78] The Government has brought forward legislation that criminalises the taking of intimate images (creation) without consent,[79] but the need to address possession, and therefore ensure that the same duties apply for NCII as for CSAM, is so far unmet.[80] In written evidence, Microsoft confirmed the different level of duties on providers:

> The current state of the criminal law also has flow-on impacts for provider duties under the OSA. The OSA and the draft Illegal Content Code of Practice ("draft Code") oblige regulated services to have systems and processes in place to limit illegal behaviours and access to illegal content through those services. Importantly, regulated services will be required to assess the risk of misuse for both CSAM and NCII harms and to take steps to mitigate both risks. However, the recommended mitigations in the draft Code necessarily differ, given how the related criminal offences vary.
>
> Because NCII content creation and possession are not illegal, the draft Code would not address the content but rather the conduct–to wit, sharing or communicating threats to share NCII. User-to-user services would be expected to have systems and processes in place to limit the risk of NCII sharing, or threats of NCII sharing, through the service (noting that search services do not generally offer sharing mechanisms) but not to take steps (for example) to address risks related to the creation of NCII.[81]

56. **CONCLUSION**
For internet infrastructure providers to take the threat of NCII seriously and block access to websites that refuse to take it down, we believe that there is justification in bringing NCII in line with CSAM in law.

78 Microsoft, [IIA0010]
79 Crime and Policing Bill 2025, Schedule 8
80 Microsoft, [IIA0010]
81 Microsoft, [IIA0010]

57. **RECOMMENDATION**
The Government should bring forward an amendment to the Crime and Policing Bill to make possession of NCII an offence, in addition to its creation. This will put NCII on the same footing as CSAM in how it is treated online and—we hope—will provide the necessary encouragement to IIPs to block or disrupt access to such content, including that which is hosted overseas.

58. **RECOMMENDATION**
The Government should create guidance for internet infrastructure providers and web browser manufacturers on tackling online non-consensual intimate image abuse, similar to that which already exists for online child sexual exploitation and abuse. This guidance should direct both groups to make use of a designated expert body's registry of NCII material. While there is no legal obligation to act in accordance with the guidance—and we understand the current voluntary approach with CSAM is working—the Government should do all it can to encourage companies to follow it, with a view to potential legislative solutions if there is insufficient take up.

59. **RECOMMENDATION**
In its illegal content Codes of Practice, Ofcom should direct user-to-user and search engine services to make use of a registry of NCII content, compiled by an expert body, on a similar basis to the provisions that exist for child sexual abuse material.

Solicitation of NCII, including from perpetrators based overseas

60. In September 2024, Baroness Owen of Alderley Edge introduced a Bill in the House of Lords that would have made the creation and solicitation of NCII criminal offences. The Bill did not receive Government support. On solicitation, the Government argued that there was no need for a specific offence on the grounds that "for every offence, except those that are specifically excluded, it is automatically also an offence to encourage or assist that offence".[82]

61. During debate on second reading of Baroness Owen's Bill, concern was raised about how the Government's argument—that the offence of solicitation already existed—applied to the solicitation of images where the creator of the image is not known or is based overseas, particularly with

82 HL Deb, 13 December 2024, col 2040

regard to synthetic content (deepfakes).[83] Misunderstanding of the law on solicitation on the part of the police was also raised with us as a concern that needed addressing by the introduction of specific offence.[84]

62. Addressing this is urgent; for example, a recent report found networks of men using peer-to-peer internet message boards to order, share and trade explicit images of women in their local area.[85] A campaigner named Jodie, who we are very grateful to for meeting with us privately, has called publicly for the law to be changed after a former friend was convicted of sharing deepfake images of her that he had asked others to create.[86] Speaking to Jodie made clear to us the importance of a specific offence on solicitation of intimate images.

63. For a new offence to be effective, Professor McGlynn and Professor Gemma Davies explained that the Government should make it an offence to solicit the image, regardless of the location of the person requested to make it, and regardless of whether it is known which person was in fact assisted and encouraged.[87] As well as closing an otherwise "significant gap in the law", they argued that creating a specific offence of soliciting would "make it clearer to perpetrators and the police that it is a criminal offence to request someone else create a sexually explicit image".[88]

64. The Government has since accepted the need to address concerns relating to the solicitation of the creation of sexually explicit deepfake images without consent and the Data (Use and Access) Bill has been amended accordingly, with the Government noting that further work on this clause might be required. However, a gap remains on the solicitation of the taking of non-synthetic intimate images.

65. **RECOMMENDATION**

The law on solicitation was unclear, incomplete and open to misinterpretation by law enforcement agencies and others. We welcome the Government's proposals to introduce a specific offence of solicitation for synthetic content via an amendment to the Data (Use and Access) Bill. We urge the Government to expand this clause to include all image-based abuse offences, maintaining a focus on criminalising the person in the UK soliciting the image, regardless of the jurisdiction and identity of the provider.

83 HL Deb, 13 December 2024, col 2042
84 Professors Gemma Davies and Clare McGlynn, [IIA0012], s 30
85 The Guardian, Online forums being used to trade explicit images of local women, 14 Feb 2025
86 BBC News, 'I was deepfaked by my best friend', 2 April 2024
87 Professors Gemma Davies and Clare McGlynn, [IIA0012], s 26–28
88 Professors Gemma Davies and Clare McGlynn, [IIA0012], s 30

New civil law to complement the criminal law pertaining to NCII abuse

66. Written evidence we received from legal experts argued that a comprehensive legislative response to NCII must include a specific "statutory civil right of action for intimate image abuse, together with civil orders".[89] Doing so would follow the precedent of numerous states in the USA and provinces in Canada—the regime in British Columbia being a good example, where such orders are inexpensive and can be produced quickly. These orders enable survivors to have their images removed or blocked online, secure compensation, and require the perpetrator to delete the content.[90]

67. A civil regime has the potential to reduce the burden on the criminal justice system by providing complementary and swifter avenues for victims to pursue redress, especially those who, understandably, might not wish to report what has happened to them to the police.[91] Formal 'Take Down' court orders sent by a designated body may also be more likely to induce action by non-compliant sites than requests from NGOs and individuals.

68. We asked the Government if they would consider implementing new civil law legislation for a statutory regime on NCII. Minister Davies-Jones told us that:

> There are already a wide range of civil actions that can be taken against those who are perpetrating intimate image abuse, including actions for defamation and harassment. Victims and survivors are able to get that redress directly from the perpetrator.[92]

89 Professor Clare McGlynn and Professor Lorna Woods [IIA003] para 8

90 Professor Clare McGlynn [IIA0005] pg 6 para 87; Civil Resolution Tribunal, Intimate Images, accessed 20 Feb 2025; The Intimate Images Protection Service in British Columbia describes its functions as including:" Providing emotional support and resources; Sharing information about your legal rights and options; Helping you apply to the Civil Resolution Tribunal (for an Intimate Images Protection Order asking platforms/ people to remove or delete intimate images shared without your consent); Sending Intimate Images Protection Orders to online platforms and/or people who have shared your image without consent; Providing information about options for enforcing Protection Orders (e.g., administrative penalties); Sharing other strategies for getting your image removed (reporting to social media platforms, 'deindexing' images to remove search, etc.); and Connecting you with other helpful services and supports"

91 Professor Clare McGlynn and Professor Lorna Woods [IIA003] para 38

92 Q120

69. The Government wrote to us setting out the civil actions that could be taken against perpetrators. However, evidence we received suggested that these options, such as misuse of private information and defamation claims, are confusing, complex, and largely inaccessible due to the cost and need for specialist legal advice.[93] [94]

70. Several stakeholders advocated for the Government to create a statutory civil regime.[95] This could follow the precedent of the Protection of Harassment Act 1997, which includes both civil and criminal remedies.[96] Such a regime would set out the orders that can be granted, including, for example, the power for content to be designated as NCII and added to a dedicated registry of NCII content, which internet infrastructure providers should be required to take note of.

71. **RECOMMENDATION**

The Government should take a holistic approach to legislating against NCII abuse by introducing a swift, inexpensive statutory civil process, as has been established in other jurisdictions such as British Columbia in Canada. Doing so would recognise survivors' wishes to access redress beyond the criminal law, as well as empower them to take fast and effective action towards having their NCII taken down or blocked. Such a regime should be alongside and underpin the creation of a registry of NCII content—overseen by an expert body—that internet infrastructure providers are requested to take all reasonable steps to prevent access to. The statutory regime should enable civil courts to make orders, including:

a. designating an image as NCII content and ordering its inclusion on a dedicated registry for the purposes of having IIPs take action to prevent access to that content;

b. prohibiting the individual from distributing the intimate image;

c. requiring the individual to delete any images;

d. requiring the individual to take down or disable access to an intimate image;

93 Correspondence from Parliamentary Under-Secretary of State, MoJ & Parliamentary Under-Secretary of State Home Office: Clarifying the law on intimate image abuse, 20 Dec 2024, para 24–28;

94 Professor Clare McGlynn [IIA0005] pg1 para 76

95 End Violence Against Women Coalition #NotYourPorn, Glamour UK, Professor Clare McGlynn, Stop Image-Based Abuse, September 2024; Professor Clare McGlynn [IIA0005]; Professor Clare McGlynn and Professor Lorna Woods [IIA003]

96 End Violence Against Women Coalition #NotYourPorn, Glamour UK, Professor Clare McGlynn, Stop Image-Based Abuse, September 2024; Professor Clare McGlynn and Professor Lorna Woods [IIA003] para 31

e. requiring the individual to pay compensation for harm caused;

f. requiring the provider and/or end user of a social media service, relevant electronic service or designated internet service to remove an intimate image from the service;

g. requiring a hosting service provider who hosts an intimate image to cease hosting the image.

Creation of an Online Safety Commission to empower victims of NCII abuse

72. As discussed earlier in this Report, Ofcom's enforcement powers are slow and ill-suited to the dynamic threat posed by NCII abuse online, particularly when hosted on non-compliant websites. Ofcom also lacks the ability to support individual victims of NCII abuse; its online complaints portal makes clear that "Ofcom is not able to respond to or adjudicate on individual complaints" and that "the information [provided] will help us monitor whether online services are complying with their online safety obligations".[97]

73. In contrast, for years other countries have tackled the issue of online harms—and NCII abuse particularly—with regulatory bodies that are focused on online safety. Professor McGlynn argued that these bodies have been far more effective at tackling NCII abuse than current UK regulatory processes.[98] For example, the Australian eSafety Commissioner can bring cases and contact platforms on behalf of individual victims of NCII abuse, working in conjunction alongside law enforcement agencies.[99] The Commissioner is also able to direct Australian ISPs to block certain content.[100] Other examples of best practice include New Zealand's Netsafe, South Korea's Advocacy Centre for Online Sexual Abuse Victims and, at a province-level, British Columbia's Intimate Images Protection Service.[101]

74. To close this enforcement gap, several stakeholders advocated the creation of an online safety commission in the UK—a dedicated body to champion the rights of victims and survivors of online abuse that can hold tech companies to account.[102] Asked whether such a body should be set up in the UK, the Minister told us:

97 Ofcom, Complain to Ofcom, (accessed 10 Feb 2025)
98 Professor Clare McGlynn [IIA0005] pg8 para 111
99 eSafety Commissioner, An overview of eSafety's role and functions, July 2021
100 eSafety Commissioner, An overview of eSafety's role and functions, July 2021
101 Professor Clare McGlynn, Professor Erika Rackley, Assistant Professor Kelly Johnson, Shattering Lives and Myths: A Report on Image-Based Sexual Abuse, 1 July 2019
102 EVAW Coalition #NotYourPorn, Glamour UK, Professor Clare McGlynn, Stop Image-Based Abuse, September 2024; Professor Clare McGlynn and Professor Lorna Woods [IIA003]; Evidence submitted in confidence for survivors of NCII abuse

> We have the Victims' Commissioner and the Domestic Abuse commissioner. There are a number of commissioners where victims and survivors can go to get support already and we would not want to be diluting their roles, voices and core purpose[103]

However, Professor McGlynn pointed out that the Online Safety Commission would be "different from the roles of the Victims Commissioner, Domestic Abuse Commissioner and similar", arguing that the Online Safety Commissions in Ireland and Australia would be a better comparison.[104]

75. **CONCLUSION**
There is a gap in the UK's online regulatory framework for a statutory body to support and champion the rights of individuals affected by non-consensual intimate image abuse, and to work alongside the courts in the civil regime. Such a body is required to help ensure victims are able to secure redress and to oversee the registry of NCII content that we recommend is introduced. Ofcom's remit is already very wide, and its enforcement mechanisms are designed to act at too a high level for this function - it is ill-suited to the further responsibilities that are required. Existing Commissions, such as the Victims' Commissioner for England and Wales, do not have the powers or expertise to fulfil such a role.

76. **RECOMMENDATION**
The Government should set up an Online Safety Commission, similar to the eSafety Commission in Australia, with a focus on support for individuals. The new Commission would act as a trusted flagger of NCII content on behalf of individuals that report it to them. The Commission would be able to apply for and send court orders, generated following a statutory civil process, for example demanding that NCII content is taken down from the websites hosting it. The Commission would oversee a registry of designated NCII content, against which it would be able to recommend that internet infrastructure providers—including ISPs, web browsers, registries, and Mobile Network Operators and others—take steps to block access to NCII content.

103 Q130 [Alex-Davies-Jones]
104 Professor Clare McGlynn [IIA0005] pg 8 para 113–4

77. **RECOMMENDATION**
The UK already has an excellent organisation doing some of this work in the form of the Revenge Porn Helpline. The Government should discuss the proposals set out above with the RPH to determine what relationship the RPH could have with the proposed Commission, or—preferably, given the expertise at the RPH—whether it can be given additional resources to take on the role of the Commission itself. The removal of images should still be pursued at the earliest opportunity as happens now; the court process that we suggest is a means of escalation in cases of non-compliance.

78. **RECOMMENDATION**
The Government should explore whether the funding for such a Commission could be generated, at least in part, by a levy on bodies within scope of the OSA on a similar basis to that which exists in other regulated environments. We note that such consideration would need to take into account fees already collected by Ofcom.

Culturally intimate images

79. NCII does not only refer to sexually explicit content; David Wright explained that in some countries and communities:

> based on culture, based on religion, just merely being photographed or taken in an image with your arm around somebody has catastrophic implications for them. That is why we refer to non-consensual intimate image abuse, not non-consensual sexual image abuse.[105]

80. At the same oral evidence session, OnlyFans CEO Keily Blair stated that the issue of culturally intimate images is why they consider consent to be the key decider of whether an image should be taken down:

> The point that David makes is a thoroughly excellent one and shows the lack of understanding by some of the other platforms that he referred to earlier where they are simply talking about preventing nudity.
>
> It is a lack of understanding about intimacy in different social contexts and that is why, for us, the key issue is consent. The people featured in the image have to consent to being in the image.

105 Oral evidence taken on 8 May 2024, Q64

> If somebody raises to us a picture of them entirely fully clothed but in a compromising position culturally or, for example, maybe not wearing a hijab or something along those lines, we would absolutely take that image down. It does not need to be sexual in nature for us to act.[106]

81. Sophie Mortimer, manager of the Revenge Porn Helpline, said she did not think the OSA covered non-sexual, culturally intimate images as NCII:

> To your example of a woman without a hijab where there will be an expectation that she will be wearing one, that image would not necessarily be classed as an intimate image, certainly not under the legislation that the Revenge Porn Helpline works under.[107]

82. Minister Alex Davies-Jones referred to the Law Commission's decision not to recommend that images other than those that are sexual, nude, partially nude or toileting were included in the criminal offence of taking or sharing intimate images:[108]

> This is a complex area […] We need to be very clear that what counts as intimate for one person can be very different for someone else. It can also be different between different communities and groups.
>
> The Law Commission has already looked at this and concluded that it would be impossible to craft a definition that suits everyone and that therefore it could result in overcriminalisation.
>
> However, where such images are uploaded, they could be caught under existing offences, such as blackmail or harassment. But we are keeping this area of law under review and will not hesitate to act if there are gaps.[109]

83. Professor Clare McGlynn advocated the adoption of the Australian civil law regime's approach to this issue, as per Section 9B of the Enhancing Online Safety Act 2015. Professor McGlynn argued that this would at least ensure that images that are generally considered to qualify as NCII for religious reasons are defined by law as being intimate. In the Australian civil law, intimate images are defined as including those where:

> because of the person's religious or cultural background, the person consistently wears particular attire of religious or cultural significance whenever the person is in public; and the material depicts, or appears

106 Oral evidence taken on 8 May 2024, Q65
107 Q22
108 Law Commission, Intimate Image Abuse: Summary of the Final Report, 2022
109 Q138

to depict, the person: (a) without that attire; and (b) in circumstances in which an ordinary reasonable person would reasonably expect to be afforded privacy.[110]

84. Professor McGlynn and her colleagues recommended that the Law Commission adopt the Australian provisions for the criminal context in England and Wales, but replace 'consistently' with commonly or usually. This would then "include images that have the potential to cause significant harms".[111] By being "specific to the cultural or religious context", it was argued that this approach would not rely on "extending the scope of the law on 'private' or intimate images more generally", therefore avoiding the "risk of overcriminalisation that may come with a broader definition".[112]

85. **CONCLUSION**
Non-consensual intimate image abuse is not always limited to sexually explicit content. For example, in some cultures, countries, or religions, sharing a photograph of someone without their religious clothing—or with their arm around another person—can be disastrous for the victim.

86. **RECOMMENDATION**
The Government should extend the legal definition of an intimate image to include images where "because of the person's religious or cultural background, the person commonly wears particular attire of religious or cultural significance when in public; and the material depicts, or appears to depict, the person: (a) without that attire; and (b) in circumstances in which an ordinary reasonable person would reasonably expect to be afforded privacy".

Statutory time limits applying to summary only intimate-image abuse offences

87. Where an offence is a summary only offence (i.e. the case can only be tried in a magistrates' court), a statutory time limit of six months applies.[113] This is the time within which a prosecution must be commenced after the offence is committed.

110 Professor Clare McGlynn [IIA0005] pg 8 para 101–4
111 Professor Clare McGlynn [IIA0005] pg 8 para 105
112 Professor Clare McGlynn [IIA0005] pg 8 para 107
113 Magistrates' Court Act 1980, section 127(1)

88. The offence of sharing NCII is a summary only offence.[114] The creation offence for deepfakes, that the Government had initially proposed adding to the Data (Use and Access) Bill currently progressing through Parliament, and the Government's proposed taking of NCII "base" offence (i.e. the offence that does not requiring determination of a specific motivation on the part of the perpetrator), are also summary offences.[115]

89. However, many victims of image-based abuse do not become aware of the abuse until after six months. It is not unusual for women and girls to find out about the abuse many months, even years, after material has been taken and/or shared online without their consent. This is especially so where material is created and/or shared in online forums or private groups.[116]

90. If the statutory time limit remains in place for these offences, many victims will be denied justice. While there are more serious intimate-image offences to which the time limits do not apply, these require the determination of specific motivations on the part of the perpetrator, for which there is often a lack of evidence.[117] Indeed, the activist organisation #NotYourPorn, which supports survivors and advocates for better laws and policies to prevent and reduce the harms of NCII abuse, has supported survivors who did not become aware of the abuse until six months or more after it was shared.[118]

91. The Government has accepted the need to reform the applicability of the time limit in these cases, proposing that the time limits should start from when the police are made aware of the abuse.[119] However, Professor of Law Clare McGlynn wrote to us saying that it was:

> very easy to imagine a scenario in which the police become aware of possible abuse but fail to identify and/or notify the victim, and/or fail to take the necessary action within the time scale required.[120]

92. We heard from several survivors of NCII abuse in confidence; one told us of an instance whereby police had failed to notify some of the other victims of her case, despite the police having already been given many of the victims' details. These women only found out that they were victims when contacted by a journalist after the perpetrator had been convicted. Another such survivor described being told that the time limit in her case had passed as having "a devastating impact on me as a victim."[121]

---

114 Professor Clare McGlynn [IIA0015] para 2
115 Professor Clare McGlynn [IIA0015] para 3–4
116 Professor Clare McGlynn [IIA0005] para 5
117 Professor Clare McGlynn [IIA0005] para 6
118 Professor Clare McGlynn [IIA0005] para 7
119 Professor Clare McGlynn [IIA0005] para 11
120 Professor Clare McGlynn [IIA0005] para 12
121 Anonymised (IIA0013)

93. **RECOMMENDATION**

The Government should introduce an extension to the statutory time limits that apply to current and forthcoming intimate image abuse offences, such that the time limit begins only once the victim(s) is/are aware of the abuse.

4 Police response to non-consensual intimate imagery

Police response to reports of non-consensual intimate image abuse

94. Georgia Harrison described to us the importance of the initial response from the police, when a victim comes forward to report NCII abuse:

> It is very important that police are aware that when they are coming to them, they are still going to be feeling such an array of emotions: shame, blame, all these things. So it is important that they do not say anything that can trigger them at that point, because that is where they will then feel like they need to retract. So if someone did have training on how to handle this emotion, what to say and what not to, I think more people would proceed forward with their claim.[122]

Georgia explained that while she had a "very good response" from Essex Police when she reported her case of NCII abuse, she is regularly contacted by other victims of NCII abuse, and acknowledged that not everyone has such a positive experience:

> So many victims give up during the process because it is just too much for them, or they are not sure if they are doing or saying the right thing. Sometimes they feel like they are getting victim blamed […] judged because they allowed the video or picture to be taken. There should be no element of judgement for that because that is not breaking the law […] breaking the law is sharing it without consent, and it is definitely important that police are aware of that[123]

95. Concern about survivors' experiences with the police was reiterated by David Wright, Chief Executive of SWGfL and Director of the UK Safer Internet Centre:

122 Oral evidence taken on 8 May 2024, Q26
123 Oral evidence taken on 8 May 2024, Q8; Q24

> I hear what Georgia [Harrison] said about Essex Police and that is wonderful; it is great that she had that experience. That is not generally our experience in terms of the victims that we support from a Revenge Porn Helpline perspective. We spend a lot of time coaching victims who have contacted the police and reminding them that, "Yes, you are a victim of a crime. You need to go back and you need to report this. This is how you do it." It is frustrating that we have to expend time doing that.[124]

96. The Revenge Porn Helpline's manager, Sophie Mortimer, told us that the majority of people that they support have had a negative experience when reporting NCII abuse to the police:

> We record people's responses to how they have been dealt with by the police where they have already gone to the police before we speak to them.
>
> Of the people who went to the police, four times as many reported a negative experience of reporting as opposed to a positive one, and that largely comes down to the officer or the call handler—the first person they have interacted with—around their understanding of the law as it is written in both its incarnations, how it might apply to their case, and what can be done to support them.
>
> The sense that many victims come away with is that there is no help, that their content cannot be removed from the internet, that perpetrators are rarely prosecuted and even more rarely convicted, and that there will be no just outcome for them.[125]

97. The UK charity Glitch, who work to end online abuse, described victims and survivors as being "re-traumatised by police" when reporting online abuse.[126] Survivors of NCII abuse that we spoke to in confidence told us that they felt the police did not care about them, citing experiences including:

- being made to feel as though they were the ones on trial during police questioning;
- evidence they submitted being lost, including having to be relive their abuse because of police interview recordings being lost;
- feeling as though they were being intimidated into dropping their case because they were wasting police time;

124 Oral evidence taken on 8 May 2024, Q65
125 Q3
126 Glitch, Laws Don't Prevent Harm: 5 Things That Will Protect Women from Deepfake "Porn", accessed 14 Feb 2025

- telling the police of other victims of their abuser who the police did not then inform;
- in one case, being referred to by an officer as a "prostitute".[127]

98. Sam Millar, Assistant Chief Constable and Strategic Programme Director of the VAWG Taskforce at the National Police Chiefs Council, described the scale of the problem of police treatment of NCII abuse victims:

> yesterday, a victim said to me that she is in a conversation with 450 victims of deepfake imagery, but only two of them had had a positive experience of policing. It is deeply worrying with those victims.[128]
>
> […] Having spent three years hearing the testimonies about what a poor service the frontline often is, I am absolutely clear that we must learn from what we have seen.[129]

Lack of adequate infrastructure within police to deal with the needs of the upcoming legislation

99. ACC Sam Millar referenced the role of system failings in explaining the poor treatment that victims faced when reporting NCII abuse to the police:

> The fact that [victims] turn up to that poor service means that our system—this is not individual police officers, but the system—is failing to put in the knowledge, the mindset, the specialist understanding or a response to legislation, which is pretty difficult for a generic police officer to keep in their mind.[130]

She described a lack of infrastructure within the police to guide and support officers in responding to reports of NCII abuse and a lack of understanding of the relevant new legislation in the Online Safety Act.[131]

100. The Revenge Porn Helpline told us that sometimes they would be asked by the police not to take down a victim's NCII so that it would remain online during their court case.[132] In response, Sam Millar referenced the lack of an investigation model for police to follow:

127 Q147
128 Q76
129 Q81
130 Q76
131 Q76
132 Q29

> A new operating model needs to set out what a good investigation looks like, because it cannot be right that officers are failing to understand that by keeping an image online, it is just constantly retraumatising […] There are plenty of occasions when we do take the content down and then the investigation starts, but it is that inconsistency of practice that we have to put right[133]

Sam Millar told us that policing needs to take VAWG and related offences more seriously, to the same extent as other crimes: "you need to invest in it and you need to help policing to build the capability.[134]

101. Professor Clare McGlynn, an expert on image-based sexual abuse, likened the police's failings in this area as being similar to those addressed by Project Soteria, a police programme to develop new operating models for the investigation and prosecution of rape in England and Wales, which started in 2021.[135] The project and resultant "National Operating Model" was developed through collaboration between academics (including Professor McGlynn), the police, and those with experience of working with and supporting survivors. A similar approach, McGlynn argues, will lead to improvements with NCII abuse:

> Image-based abuse is distinct and a similar approach is required to ensure that the experiences of both working with and reporting to the police are integrated into any new guidance and training. There is already guidance and training being developed as part of the policing response to the Angiolini Review. The guidance and training on non-contact sexual offences includes some forms of image based abuse such as voyeurism, taking and sharing intimate images.[136]

102. The Government told us that they are committed to playing a "more active role in policing to ensure officers have the right support, to significantly improve standards across the board and to ensure justice is delivered for victims."[137] Given that VAWG was a part of the "Strategic Policing Requirement", the Government argued that forces must therefore treat it as a national priority, like terrorism and child sexual abuse, adding that:

133 Q79
134 Q79
135 Professor Clare McGlynn [IIA0005] pg 7 para 94–95
136 Professor Clare McGlynn [IIA0005] pg 7 para 98–97
137 Correspondence from Parliamentary Under-Secretary of State, Ministry of Justice & Parliamentary Under-Secretary of State Home Office: Tackling non-consensual intimate image abuse, 20 Dec 2024

> We expect to see sustained work across policing to drive up standards and to ensure there is always a swift and specialist response to these appalling crimes.[138]

They also cited the College of Policing "developing evidence-based guidance and training in handling and investigating non-contact sexual offences for first responders, call handlers, investigators and supervisors."[139]

103. **CONCLUSION**
Every victim of a sexual offence deserves to be treated with respect and have their case investigated promptly and effectively by the police. However, in many cases police treatment of victims of intimate image abuse has been characterised by a lack of understanding and in some cases misogyny, with officers' choosing to patronise victims rather than support them. This is unacceptable and must change.

104. **RECOMMENDATION**
The College of Policing, Ofcom, and the Revenge Porn Helpline should work together to produce guidance to improve the police response to reports of non-consensual intimate image abuse. That guidance should include the steps police officers need to take to help ensure that content is taken down and blocked as a matter of priority.

Deprivation of material

105. In evidence to the Committee, Sophie Mortimer referenced a victim of NCII abuse whose content was shared in her workplace by an ex-partner (who had captured the material without her knowledge). Despite the accused pleading guilty and receiving a suspended sentence and restraining order, he had the device containing the NCII (which had been seized by the police) returned to him. Sophie Mortimer explained:

> [The Police] said, "Our hands are tied,"
>
> … the orders available to magistrates and judges to deal with this are not designed for devices and the content on the device or additional forms of storage such as iCloud storage. The mechanisms have not

138 Correspondence from Parliamentary Under-Secretary of State, Ministry of Justice & Parliamentary Under-Secretary of State Home Office: Tackling non-consensual intimate image abuse, 20 Dec 2024

139 Correspondence from Parliamentary Under-Secretary of State, Ministry of Justice & Parliamentary Under-Secretary of State Home Office: Tackling non-consensual intimate image abuse, 20 Dec 2024

been put in place or utilised.[140]

Campaigners described the current situation as leaving victims of NCII abuse "living in fear" that the images could be shared again. Elena Michael, of the campaign group #NotYourPorn, said it was like "handing back the weapon that caused the crime and rolling out the carpet for them to do it again".[141]

106. We asked the Minister why perpetrators were having the content returned to them. She told us that, in fact, this could be prevented: "the courts do have the power under certain sections of the Sentencing Act [section 153] to seize these devices used for the purposes of or for facilitation of the commission of the criminal offence."[142] Following the session, the Minister wrote to us reiterating that the Courts have that power:

> Where a person is convicted of sharing or threatening to share an intimate photograph, the Court would therefore have the power to deprive the offender of laptops or mobile phones used for committing these offences, or which the offender intends to use to commit further offences, as well as the images themselves. Section 153 also gives the Court the power to deprive an offender of property where the possession of the property is in itself an offence.
>
> We do not have data on the use of deprivation orders in sentencing for intimate image abuse offences.[143]

107. On 22 February 2025, an Observer analysis of magistrates' court records of NCII cases found that of the 98 intimate image abuse cases concluded in the in last six months, just three resulted in a deprivation order.[144] 54 of those cases were sufficiently serious to merit restraining orders.

108. The Government told us: "The Sentencing Council is currently reviewing their guidance on ancillary orders, including deprivation orders, to improve its clarity, accuracy and usefulness to sentencers. The consultation closed on 4 December."[145] The Crime and Policing Bill introduces changes to the

140 Q19
141 The Observer, 'Revenge porn' abusers allowed to keep devices with explicit images, 22 Feb 2025
142 Q107
143 Correspondence from Parliamentary Under-Secretary of State, Ministry of Justice & Parliamentary Under-Secretary of State Home Office: Tackling non-consensual intimate image abuse, 20 Dec 2024
144 The Observer, 'Revenge porn' abusers allowed to keep devices with explicit images, 22 Feb 2025
145 Correspondence from Parliamentary Under-Secretary of State, MoJ & Parliamentary Under-Secretary of State Home Office: Clarifying the law on intimate image abuse, 20 Dec 2024, para 23

Sentencing Code to make clear that when a person commits one of the new taking offences, the photograph or film or anything containing it can be subject to a deprivation order if the criteria is met.[146]

109. **CONCLUSION**
Cases have been drawn to our attention where, at the end of the criminal justice process, perpetrators have had the devices containing the NCII content returned to them—even in cases where the perpetrator has been served with a restraining order. It is needless for us to say how harrowing that must be for the victims of these crimes. It is staggering that the criminal justice system has allowed this to occur. The measures in the Crime and Policing Bill to make clear that perpetrators found guilty of the new offence of taking NCII can be deprived of that content are very welcome. However, they may not address concerns that people found guilty of sharing that content are not being deprived of the material.

110. **RECOMMENDATION**
The Sentencing Council must take steps to increase awareness of the ability of the courts to ensure that those charged with NCII offences forfeit all right to continued possession of that material, including both the physical removal of devices on which that material may be stored and deletion of any content stored remotely. In response to this report, the Crown Prosecution Service should also set out what action it will take to stop perpetrators of NCII abuse from retaining that content. The Government should collect data on the use of deprivation orders in NCII cases so that it can satisfy itself and others that the criminal justice system is taking seriously the impact on victims of perpetrators retaining the control of the harmful content.

NCII as part of the national mission to reduce VAWG by 50%

111. The Government has declared VAWG to be a national emergency and announced a mission to cut it by 50% within the next decade.[147] However, a report by the National Audit Office (NAO) found that the "lack of a consistent definition for VAWG across public bodies and their approaches to measuring the scale of VAWG crimes has made it difficult to measure progress".[148] Furthermore, they found that "the Home Office has made little progress

146 Crime and Policing Bill 2025, Schedule 8 Part 2
147 Labour Party website, Yvette Cooper speech at Labour Party Conference 2024, (accessed Sept 24 2024)
148 National Audit Office, Tackling violence against women and girls, January 2025 pg 7

developing measures to prevent VAWG", and recommended that they should agree "a common definition of VAWG across government and policing and identifying the data that will be used to measure this".[149]

112. **RECOMMENDATION**
The Government should ensure that NCII abuse is included when creating a common definition of VAWG, as part of its mission to reduce it by 50% within the next decade. It should also identify what data can be used to measure the specific prevalence of NCII, as part of that mission.

149 National Audit Office, Tackling violence against women and girls, January 2025 pgs 9–10

5 The use of preventative technology

113. In 2021, the Revenge Porn Helpline, operated by SWGfL, launched StopNCII.org, a free 'hashing' tool designed to protect people threatened with NCII abuse.[150] David Wright explained how the tool works:

> say you are being threatened—any adult globally—you visit the website on your device; you create what is called a hash, a digital fingerprint that uniquely identifies the image or video that you have on your device […] [the image] never leaves their device. It is the hash code, a digital fingerprint, that is then added on to the StopNCII dataset, and we then distribute that to participating platforms as a signal to enable them to prevent that image or video from being posted on their platform.[151]

114. One of the particular 'selling points' of StopNCII.org's hashing technology is that using a hash means that the victims retain control of the content, which never has to leave their device. The tool is to *prevent* content being uploaded, so it might not actually be online yet; if victims had to upload their content to a website, thus giving control of the image to a third party, this might dissuade them from using the tool.

115. The technology was developed with Meta and launched in December 2021. As of February 2025, 13 platforms are listed on StopNCII.org as accepting their hashes: Facebook, Instagram, Threads, Microsoft Bing, TikTok, Reddit, OnlyFans, Snap Inc, Niantic, playhouse, Redgifs, Bitly and Pornhub.[152] David Wright told our predecessors that:

> Over 970,000 hashes have been created by individuals over the nearly three years since StopNCII began. When a platform identifies a match—that somebody is trying to upload that image—it invokes their normal moderation processes, whether automated or human. They then get to view the image or the video. If it is NCII, they will then add a tag on to that hash, which then goes back into the system. The hash does two things: first, it provides information to all the other

150 SWGfL, 'Revenge Porn Helpline and SWGfL announce the launch of StopNCII.org', accessed 22 May

151 Oral evidence taken on 8 May 2024, Q29

152 StopNCII, Industry Partners, accessed 17 February 2025

> platforms that this is now a verified hash; and, secondly, it indicates to us how many times StopNCII has actively worked. Currently, we are working at about 22,000 instances […].[153]

116. We asked the CEO of OnlyFans, an online content subscription service, if the process of joining the StopNCII initiative presented any issues or difficulties. She told us:

> we started the implementation in January. We finished the first phase of the implementation the same month. It took approximately 80 hours of tech and engineering time to be able to fully integrate phase 1. Phase 2 was implementing the feedback loop, which is enabling us to actually provide feedback to StopNCII about hash matches and things like that. That took a little more time; that was more complex; and that was fully implemented by the end of March. In terms of monthly maintenance hours, I would say, typically, between four and five hours a month of dev and tech time, a little legal advice from time to time comes into things when there is contracting to do, but it is not an overly onerous process.[154]

WEC correspondence with platforms that had not partnered with StopNCII

117. In March 2024, our predecessors wrote to several technology and social media platforms, asking why they did not accept StopNCII.org hashes.[155] Several agreed to meet or work towards partnering with StopNCII, including X,[156] Patreon[157] and Discord.[158] Others were supportive but felt that StopNCII hashing wouldn't be effective or applicable in their specific platform's context.[159]

153 Q8
154 Oral evidence taken on 8 May 2024, Q36
155 Correspondence from the Chair of the previous committee to various major platforms, dated 28 March 2025
156 Correspondence from X relating to non-consensual intimate image abuse, dated 25 April
157 Correspondence from Patreon relating to non-consensual intimate image abuse, dated 29 April
158 Correspondence from Discord relating to non-consensual intimate image abuse, dated 10 April
159 Correspondence from Zoom, relating to tackling NCII abuse, dated 4 April 2024; Correspondence from Pinterest, relating to tackling NCII abuse, dated 10 April 2024; Correspondence from Discord, relating to tackling NCII abuse, dated 10 April 2024; Correspondence from Adobe, relating to tackling NCII abuse, dated 10 April 2024; Correspondence from Twitch, relating to tackling NCII abuse, dated 11 April 2024

Microsoft Bing response

118. Microsoft has been supportive of SWGfL—in March 2024 Microsoft licensed a new form of "PhotoDNA" hash-matching technology to support StopNCII's efforts. In response to our letter, they said they were "continuing our conversations with StopNCII about ways in which we can deepen our engagement".[160] In September, Microsoft announced the formation of a partnership with StopNCII:

> We have been piloting use of the StopNCII database to prevent [NCII] from being returned in image search results in Bing. We have taken action on 268,899 images up to the end of August. We will continue to evaluate efforts to expand this partnership.[161]

119. Although Microsoft has a reporting portal for NCII, the content itself must be reviewed and confirmed as violating their NCII policy before they will remove the reported links from search results in Bing and/or remove access to the content itself if it has been shared on one of Microsoft's hosted consumer services.[162] Only 41% of the 1,425 reported requests to Microsoft in July-December 2023 were "actioned" by the company, i.e. where user-generated content was removed from its services or access to it blocked."[163]

Google response

120. In response to our letter, Google detailed its actions to combat NCII:

> When image URLs that are reported via our [NCII] reporting tool are found to be violative and are subsequently de-listed, systems are in place to detect and remove duplicates of that imagery from Search. Using our own internal hashing technology, our systems detect and remove duplicates for the vast majority of [NCII] imagery reported[164]

Google is yet to partner with StopNCII, however, saying:

> We want to reassure the Committee that Google has been in regular dialogue with StopNCII since its launch. We haven't been able to join due to specific policy and practical concerns about the interoperability of the database […] We're exploring possible solutions[165]

121. In oral evidence to our Committee, Gail Kent, Director of Search for Government Affairs at Google, explained:

---

160 Correspondence from Microsoft, relating to tackling NCII abuse, dated 12 April 2024
161 Microsoft, An update on our approach to tackling intimate image abuse, 5 Sept '24
162 QQ43–46
163 Microsoft, Digital Safety Content Report, Dec 2023
164 Correspondence from Google, relating to tackling NCII abuse, dated 17 April 2024
165 Correspondence from Google, relating to tackling NCII abuse, dated 17 April 2024

> It is about that context of when an image is shared. StopNCII was set up to focus on social media and as you heard, Meta was the main collaborator. We think there are different requirements for search engines. We are absolutely delighted that Bing has managed to work through some issues and that is absolutely our intent as well, but it is around the context of when an image is shared […][166]

> […] If we have the context then it enables us to understand what exactly the search terms were; it is less the context in which it was shared, more the search context. We are not asking, "Was this an image that was taken in these circumstances?" […] We want to know the search terms used to find it, the URLs where it was found, and then the image itself. That enables us to make sure that we can deal with duplicates, because […] hash technology is really miraculous; it had a huge impact on tackling child sexual abuse, but it can be manipulated […][167]

Google did announce in Augus 2024 that it would prevent content that an individual has requested be removed from its search results from appearing in similar searches involving that person.[168]

Consultation on including hashing to prevent NCII sharing in the Ofcom Codes of Practice

122. We asked Ofcom what steps it would take to mandate platforms to adopt protective technologies, such as the StopNCII.org tool, that have proven to be effective in safeguarding against digital violence. Dame Melanie Dawes, Chief Executive of Ofcom told us that although Ofcom's "existing consultations contain serious measures that will drive a significant improvement in user safety, they are far from the last word".[169] Dame Melanie said:

> With the Act only newly passed, Ofcom's preparations to date are necessarily being done without the benefit of information powers, and with the rapid pace of change in the industry constantly creating new risks and opportunities, [it is] clear that [it] will need to keep adapting

166 Q39
167 Q41
168 South West Grid for Learning, Google Responds to Non-Consensual Sexual Synthetic Media, 7 Aug 2024
169 Correspondence from Ofcom, relating to non-consensual intimate image abuse, dated 1 May

> and adding to [its] Codes, and quickly.[170]

As part of the publication of their Illegal Harms Codes and guidance in December 2025, Ofcom announced that they would be launching "a further Consultation in Spring 2025 on expansions to the Codes" that would include proposals on the "use of hash matching to prevent the sharing of [NCII].[171] We note that Ofcom already recommends that certain user-to-user services use hash matching technology to detect and remove CSAM content.[172] Since then, Ofcom has launched a consultation on draft Guidance regarding what platforms can do to improve the safety of women and girls online. We note that it lists hash matching against NCII as "good practice"[173] i.e. something "that providers can implement to deliver ambitious and meaningful changes towards a safer life online for women and girls".[174]

123. We asked the Parliamentary Under-Secretary of State at the Home Office, Jess Phillips, if she thought Ofcom should make accepting hashing technology a requirement for major platforms operating in the UK, she told us:

> I see no good reason why the same technology could not be used, but it will be for Ofcom to determine, following the consultation [in Spring 2025][175]

124. **CONCLUSION**

Hash matching technology is a crucial tool in preventing non-consensual intimate image abuse. It is unacceptable that so few platforms receive NCII hashes, not least when they are already able to incorporate similar technologies for preventing the sharing of child sexual abuse material. It is obvious to us that accepting hashes for NCII is the right thing to do, irrespective of whether there is legislation or statutory guidance to require it. It is disappointing that companies, in some cases trillion-dollar companies such as Google, have been unable to make that judgement. Such a company has the means to overcome any interoperability issues which currently exist.

170 Correspondence from Ofcom, relating to non-consensual intimate image abuse, dated 1 May

171 Ofcom, Overview, 16 Dec 2024

172 Correspondence with Chief Executive, Ofcom re Tackling non-consensual intimate image abuse, dated December & January 2024–25

173 Ofcom, A Safer Life Online for Women and Girls, Practical Guidance for Tech Companies para 4.41, 25 Feb 2025

174 Ofcom, A Safer Life Online for Women and Girls, Practical Guidance for Tech Companies para 1.4, 25 Feb 2025

175 Q110

125. **RECOMMENDATION**
Google should accept the StopNCII.org hash matching technology as a matter of priority.

126. **CONCLUSION**
It is clear that some companies require further persuasion to accept NCII hashes. We welcome Ofcom's plans to launch a consultation in spring 2025 on expansions to its Codes of Practice that would include proposals on the use of hash matching technology to prevent the sharing of NCII. We are clear in our view that those proposals should include requiring companies to accept the hash matching technology to prevent NCII on their services.

6 Synthetic / Deepfake NCII

127. Synthetic NCII, often referred to as 'deepfakes', refers to any sexual or nude media created using AI that represents the likeness of another individual without their consent. A form of intimate image abuse, examples of synthetic NCII can include, but are not limited to:

- the swapping of someone's face with another person's nude body.
- 'nudification' apps that alter a clothed image to make it appear nude.[176]

The harm posed by synthetic NCII

128. In 2019, even before the advent of generative AI, a report by Sensity AI found that 96% of so-called "deepfakes" were pornographic, and of those, 99% were made of women. Such images have long been used to shame, harass, and extort the person depicted, affecting not only individuals with a public profile, but also private individuals, including teens.[177]

129. Research from Graphika suggests that in September 2023 alone, there were 24 million unique visitors to synthetic NCII websites. The same report found that the number of links advertising synthetic NCII services increased more than 2,400% on social media from 2022 to 2023, and many of the services only work on women.[178] Similarly, research by My Image My Choice found over 275,000 intimate deepfake videos on the most popular deepfake sites in 2023, with a total of more than four billion views, and with more videos uploaded to these sites than in all previous years combined.[179]

176 South West Grid for Learning, Were you Affected by the Recent "Deepfake" Documentary on Channel 4?, 29 Jan 2025
177 Microsoft, Protecting the Public from Abusive AI-Generated Content, 5 November 2024
178 Microsoft, Protecting the Public from Abusive AI-Generated Content, 5 November 2024
179 My Image My Choice, Deepfake Abuse: Landscape Analysis 2023–24, February 2024

Nudification apps

130. There is also a growing problem with "nudification apps", which utilise generative AI to remove clothing from someone in an image. Multiple such apps are available, with some being "advertised on TikTok".[180] David Wright told us that:

> There should be policies and expectations—particularly on app stores—that these technologies should not be there. Back in March, we reported something like 29 different nudification app services to Apple, which then removed them, thanked us for reporting them and asked us to let them know if there were any more. Our question is: how did they get there in the first place?[181]

Government legislating against sexually explicit deepfakes

131. The Government's manifesto included a commitment to ban the creation of degrading and harmful sexually explicit deepfakes. Alex Davies-Jones, the Parliamentary Under-Secretary of State at the MoJ, explained that the Government is "looking at options to swiftly deliver that commitment in this Session of Parliament."[182]

132. Initially, the Government wrote to us to announce plans for new offences regarding the creation of deepfakes to be included in the Data (Use and Access) Bill at report stage. These offences would criminalise the creation of sexually explicit deepfakes without a person's consent, where the image had been created either for the purpose of sexual gratification or with the intent to humiliate, alarm or distress that person.[183]

133. As drafted, the amendment would have required victims to prove the perpetrator's intentions. This would have been a backward step, not least considering the Government had already removed the need to prove intent from the base sharing NCII offence.[184] A Government source told The Times

180 Sky News, AI driving 'explosion' of fake nudes as victims say the law is failing them, 6 Dec 2024

181 Q28 [David Wright]

182 HC Deb, 12 November 2024, col 187WH

183 Correspondence from Minister of State of Justice, re Tackling non-consensual intimate image abuse, dated 22 January 2025

184 The Times, Deepfake porn U-turn boosts Charlotte Owen's push for criminalisation, 25 Jan 2025; Professor Clare McGlynn [IIA0005]

that "we are minded to pursue a consent-based deepfake offence".[185] This was welcomed by campaigners, including the Head of Policy & Campaigns at End Violence Against Women noted, Rebecca Hitchen:

> This is a really welcome move from the government. The only relevant factor in sexual offending is consent and taking a consent-based approach will ensure there are no legal loopholes for perpetrators and remove some of the barriers to justice survivors face. We have seen with other offences that requiring evidence of the perpetrator's intent to harm, as well as a lack of consent, places a huge burden of proof on survivors, the police and justice system and lets perpetrators off the hook.[186]

134. **RECOMMENDATION**
The Government's plans to criminalise the creation of sexually explicit deepfakes/NCII, even if they are not shared, are very welcome and worthy of praise. However, the Government must ensure that the offence is consent-based and does not require the determination of any motivation on the part of the perpetrator. Consistent with our recommendations for non-synthetic content, the offence must also include cultural intimate image abuse, so as to include deepfakes of someone without their attire of religious or cultural significance that they commonly wear in public.

135. **RECOMMENDATION**
The private sector has innovated to create AI technology. It does not need to wait for legislation to catch up in order to safeguard individuals from harmful AI-generated content. As a starting point tech companies involved in AI content creation should cleanse their datasets of NCII content and commit to responsible sourcing of data to safeguard those datasets from being used as a base from which to create intimate image-based abuse.

185 The Times, Deepfake porn U-turn boosts Charlotte Owen's push for criminalisation, 25 Jan 2025

186 End Violence Against Women, Government U-turn on deepfakes offence, 27 Jan 2025

136. **RECOMMENDATION**

There is no legitimate reason whatsoever for the use or existence of nudification apps. The Government should ensure that the use of such an app is considered creation of synthetic NCII and therefore also a criminal offence and Ofcom should investigate the sites that offer this functionality. The Government should make sure that search engines and platforms that are found to promote or facilitate the distribution of such apps can be held to account.

Conclusions and recommendations

1. The services provided by the Revenge Porn Helpline need to be supported by sufficient funding to allow them to keep up with demand and ensure that no victim of NCII goes unsupported. Current Government funding has remained at 2020 levels despite a sevenfold increase in caseload. Future funding must increase and should be multiyear to provide a sustainable footing and allow the development of the tools necessary to help its services keep pace with the increased volume and technical sophistication of NCII abuse in the UK. (Recommendation, Paragraph 17)

2. The list of offences that are within scope of the Criminal Injuries Compensation Scheme is out of date. Crimes perpetrated online, such as non-consensual intimate image abuse, can be just as damaging to a person as those involving physical violence. They can have a catastrophic impact on a person's mental health. It is essential that victims of such crimes are able to access compensation. (Conclusion, Paragraph 25)

3. The Ministry of Justice must amend the eligibility criteria of the Criminal Injuries Compensation Scheme to bring claims from victims of sexual offences perpetrated online, specifically non-consensual intimate image abuse, within its scope. (Recommendation, Paragraph 26)

4. We welcome the inclusion in the Crime and Policing Bill of the new offences of taking an intimate image without consent and of installing equipment for the purposes of enabling the commission of those offences. We also welcome the Government's recognition that the definition of what constitutes an image for these purposes should be broad in scope - something campaigners had been calling for. These measures represent significant legislative progress in the battle to protect people from NCII abuse and punish those who commit it. (Conclusion, Paragraph 41)

5. Ofcom's current enforcement powers, while welcome, are far too slow and not designed to help individual victims get abusive images of themselves on non-compliant websites taken down or have access to them restricted. The duties under the regulatory regime created by the Online Safety Act are a good start. However, further steps are required to effectively tackle the threat posed by NCII at an individual level, particularly where content is hosted overseas. (Conclusion, Paragraph 48)

6. For internet infrastructure providers to take the threat of NCII seriously and block access to websites that refuse to take it down, we believe that there is justification in bringing NCII in line with CSAM in law. (Conclusion, Paragraph 56)

7. The Government should bring forward an amendment to the Crime and Policing Bill to make possession of NCII an offence, in addition to its creation. This will put NCII on the same footing as CSAM in how it is treated online and—we hope—will provide the necessary encouragement to IIPs to block or disrupt access to such content, including that which is hosted overseas. (Recommendation, Paragraph 57)

8. The Government should create guidance for internet infrastructure providers and web browser manufacturers on tackling online non-consensual intimate image abuse, similar to that which already exists for online child sexual exploitation and abuse. This guidance should direct both groups to make use of a designated expert body's registry of NCII material. While there is no legal obligation to act in accordance with the guidance—and we understand the current voluntary approach with CSAM is working—the Government should do all it can to encourage companies to follow it, with a view to potential legislative solutions if there is insufficient take up. (Recommendation, Paragraph 58)

9. In its illegal content Codes of Practice, Ofcom should direct user-to-user and search engine services to make use of a registry of NCII content, compiled by an expert body, on a similar basis to the provisions that exist for child sexual abuse material. (Recommendation, Paragraph 59)

10. The law on solicitation was unclear, incomplete and open to misinterpretation by law enforcement agencies and others. We welcome the Government's proposals to introduce a specific offence of solicitation for synthetic content via an amendment to the Data (Use and Access) Bill. We urge the Government to expand this clause to include all image-based abuse offences, maintaining a focus on criminalising the person in the UK soliciting the image, regardless of the jurisdiction and identity of the provider. (Recommendation, Paragraph 65)

11. The Government should take a holistic approach to legislating against NCII abuse by introducing a swift, inexpensive statutory civil process, as has been established in other jurisdictions such as British Columbia in Canada. Doing so would recognise survivors' wishes to access redress beyond the criminal law, as well as empower them to take fast and effective action towards having their NCII taken down or blocked. Such a regime should be alongside and underpin the creation of a registry of NCII content—overseen by an expert body—that internet infrastructure providers are requested to take all reasonable steps to prevent access to. The statutory regime should enable civil courts to make orders, including:

a. designating an image as NCII content and ordering its inclusion on a dedicated registry for the purposes of having IIPs take action to prevent access to that content;

b. prohibiting the individual from distributing the intimate image;

c. requiring the individual to delete any images;

d. requiring the individual to take down or disable access to an intimate image;

e. requiring the individual to pay compensation for harm caused;

f. requiring the provider and/or end user of a social media service, relevant electronic service or designated internet service to remove an intimate image from the service;

g. requiring a hosting service provider who hosts an intimate image to cease hosting the image. (Recommendation, Paragraph 71)

12. There is a gap in the UK's online regulatory framework for a statutory body to support and champion the rights of individuals affected by non-consensual intimate image abuse, and to work alongside the courts in the civil regime. Such a body is required to help ensure victims are able to secure redress and to oversee the registry of NCII content that we recommend is introduced. Ofcom's remit is already very wide, and its enforcement mechanisms are designed to act at too a high level for this function - it is ill-suited to the further responsibilities that are required. Existing Commissions, such as the Victims' Commissioner for England and Wales, do not have the powers or expertise to fulfil such a role. (Conclusion, Paragraph 75)

13. The Government should set up an Online Safety Commission, similar to the eSafety Commission in Australia, with a focus on support for individuals. The new Commission would act as a trusted flagger of NCII content on behalf of individuals that report it to them. The Commission would be able to apply for and send court orders, generated following a statutory civil process, for example demanding that NCII content is taken down from the websites hosting it. The Commission would oversee a registry of designated NCII content, against which it would be able to recommend that internet infrastructure providers—including ISPs, web browsers, registries, and Mobile Network Operators and others—take steps to block access to NCII content. (Recommendation, Paragraph 76)

14. The UK already has an excellent organisation doing some of this work in the form of the Revenge Porn Helpline. The Government should discuss the proposals set out above with the RPH to determine what relationship the RPH could have with the proposed Commission, or—preferably, given the

expertise at the RPH—whether it can be given additional resources to take on the role of the Commission itself. The removal of images should still be pursued at the earliest opportunity as happens now; the court process that we suggest is a means of escalation in cases of non-compliance. (Recommendation, Paragraph 77)

15. The Government should explore whether the funding for such a Commission could be generated, at least in part, by a levy on bodies within scope of the OSA on a similar basis to that which exists in other regulated environments. We note that such consideration would need to take into account fees already collected by Ofcom. (Recommendation, Paragraph 78)

16. Non-consensual intimate image abuse is not always limited to sexually explicit content. For example, in some cultures, countries, or religions, sharing a photograph of someone without their religious clothing—or with their arm around another person—can be disastrous for the victim. (Conclusion, Paragraph 85)

17. The Government should extend the legal definition of an intimate image to include images where "because of the person's religious or cultural background, the person commonly wears particular attire of religious or cultural significance when in public; and the material depicts, or appears to depict, the person: (a) without that attire; and (b) in circumstances in which an ordinary reasonable person would reasonably expect to be afforded privacy". (Recommendation, Paragraph 86)

18. The Government should introduce an extension to the statutory time limits that apply to current and forthcoming intimate image abuse offences, such that the time limit begins only once the victim(s) is/are aware of the abuse. (Recommendation, Paragraph 93)

19. Every victim of a sexual offence deserves to be treated with respect and have their case investigated promptly and effectively by the police. However, in many cases police treatment of victims of intimate image abuse has been characterised by a lack of understanding and in some cases misogyny, with officers' choosing to patronise victims rather than support them. This is unacceptable and must change. (Conclusion, Paragraph 103)

20. The College of Policing, Ofcom, and the Revenge Porn Helpline should work together to produce guidance to improve the police response to reports of non-consensual intimate image abuse. That guidance should include the steps police officers need to take to help ensure that content is taken down and blocked as a matter of priority. (Recommendation, Paragraph 104)

21. Cases have been drawn to our attention where, at the end of the criminal justice process, perpetrators have had the devices containing the NCII content returned to them—even in cases where the perpetrator has been

served with a restraining order. It is needless for us to say how harrowing that must be for the victims of these crimes. It is staggering that the criminal justice system has allowed this to occur. The measures in the Crime and Policing Bill to make clear that perpetrators found guilty of the new offence of taking NCII can be deprived of that content are very welcome. However, they may not address concerns that people found guilty of sharing that content are not being deprived of the material. (Conclusion, Paragraph 109)

22. The Sentencing Council must take steps to increase awareness of the ability of the courts to ensure that those charged with NCII offences forfeit all right to continued possession of that material, including both the physical removal of devices on which that material may be stored and deletion of any content stored remotely. In response to this report, the Crown Prosecution Service should also set out what action it will take to stop perpetrators of NCII abuse from retaining that content. The Government should collect data on the use of deprivation orders in NCII cases so that it can satisfy itself and others that the criminal justice system is taking seriously the impact on victims of perpetrators retaining the control of the harmful content. (Recommendation, Paragraph 110)

23. The Government should ensure that NCII abuse is included when creating a common definition of VAWG, as part of its mission to reduce it by 50% within the next decade. It should also identify what data can be used to measure the specific prevalence of NCII, as part of that mission. (Recommendation, Paragraph 112)

24. Hash matching technology is a crucial tool in preventing non-consensual intimate image abuse. It is unacceptable that so few platforms receive NCII hashes, not least when they are already able to incorporate similar technologies for preventing the sharing of child sexual abuse material. It is obvious to us that accepting hashes for NCII is the right thing to do, irrespective of whether there is legislation or statutory guidance to require it. It is disappointing that companies, in some cases trillion-dollar companies such as Google, have been unable to make that judgement. Such a company has the means to overcome any interoperability issues which currently exist. (Conclusion, Paragraph 124)

25. Google should accept the StopNCII.org hash matching technology as a matter of priority. (Recommendation, Paragraph 125)

26. It is clear that some companies require further persuasion to accept NCII hashes. We welcome Ofcom's plans to launch a consultation in spring 2025 on expansions to its Codes of Practice that would include proposals on the use of hash matching technology to prevent the sharing of NCII. We are clear in our view that those proposals should include requiring companies to accept the hash matching technology to prevent NCII on their services. (Conclusion, Paragraph 126)

27. The Government's plans to criminalise the creation of sexually explicit deepfakes/NCII, even if they are not shared, are very welcome and worthy of praise. However, the Government must ensure that the offence is consent-based and does not require the determination of any motivation on the part of the perpetrator. Consistent with our recommendations for non-synthetic content, the offence must also include cultural intimate image abuse, so as to include deepfakes of someone without their attire of religious or cultural significance that they commonly wear in public. (Recommendation, Paragraph 134)

28. The private sector has innovated to create AI technology. It does not need to wait for legislation to catch up in order to safeguard individuals from harmful AI-generated content. As a starting point tech companies involved in AI content creation should cleanse their datasets of NCII content and commit to responsible sourcing of data to safeguard those datasets from being used as a base from which to create intimate image-based abuse. (Recommendation, Paragraph 135)

29. There is no legitimate reason whatsoever for the use or existence of nudification apps. The Government should ensure that the use of such an app is considered creation of synthetic NCII and therefore also a criminal offence and Ofcom should investigate the sites that offer this functionality. The Government should make sure that search engines and platforms that are found to promote or facilitate the distribution of such apps can be held to account. (Recommendation, Paragraph 136)

Witnesses

The following witnesses gave evidence. Transcripts can be viewed on the inquiry publications page of the Committee's website.

Wednesday 8 May 2024

Georgia Harrison, Campaigner, Broadcaster and TV Personality Q1–28

David Wright, Chief Executive, SWGfL and Director, The UK Safer Internet Centre (UKSIC); **Keily Blair**, Chief Executive Officer, Only Fans Q29–67

Wednesday 6 November 2024

David Wright, Chief Executive, SWGf and Director, UK Safer Internet Centre; **Sophie Mortimer**, Manager, Revenge Porn Helpline Q1–35

Courtney Gregoire, Vice President and Chief Digital Safety Officer, Microsoft; **Gail Kent**, Director of Government Affairs and Public Policy (Search News and Gemini), Google Q36–75

Wednesday 20 November 2024

Professor Lorna Woods, Professor of Law, Essex Law School, University of Essex; **Professor Clare McGlynn**, Professor of Law, University of Durham; **Samantha Millar**, Assistant Police Chief Constable and VAWG Strategic Director, National Police Chiefs' Council Q76–103

Jess Phillips MP, Parliamentary Under-Secretary of State for Safeguarding and Violence against Women and Girls, Home Office; **Alex Davies-Jones**, Parliamentary Under-Secretary of State, Ministry of Justice; **Laura Weight**, Interim Director, Vulnerabilities & Criminal Law Policy Directorate, Ministry of Justice; **Gisela Carr**, Deputy Director of the Interpersonal Abuse Unit, Home Office Q104–154

Formal minutes

Wednesday 26 February 2025

Members present:

Sarah Owen, in the Chair

Alex Brewer

Rosie Duffield

Kirith Entwistle

Catherine Fookes

Christine Jardine

Samantha Niblett

Rachel Taylor

Tackling non-consensual intimate image abuse

Draft Report (*Tackling non-consensual intimate image abuse*), proposed by the Chair, brought up and read.

Ordered, That the Report be read a second time, paragraph by paragraph.

Paragraphs 1 to 136 read and agreed to.

Summary agreed to.

Resolved, That the Report be the Fourth Report of the Committee to the House.

Ordered, That the Chair make the Report to the House.

Ordered, That embargoed copies of the Report be made available, in accordance with the provisions of Standing Order No. 134.

Adjournment

Adjourned till Wednesday 5 March at 2.00pm.

Published written evidence

The following written evidence was received and can be viewed on the inquiry publications page of the Committee's website.

IIA numbers are generated by the evidence processing system and so may not be complete.

1	Durham University	IIA0012
2	Jodie, Image-Based Abuse Survivor-Campaigner	IIA0009
3	Kent, Gail (Global Director, Government Affairs and Public Policy, Search, News and Gemini, Google)	IIA0006
4	Kent, Gail (Global Director, Government Affairs and Public Policy, Search, News, Gemini, Google)	IIA0011
5	McGlynn, Professor Clare (Professor, University of Durham); and Professor Lorna Woods (Professor, University of Essex)	IIA0003
6	McGlynn, Professor Clare (Professor Clare McGlynn)	IIA0015
7	McGlynn, Professor Clare (Professor Clare McGlynn)	IIA0014
8	McGlynn, Professor Clare (Professor, Durham Law School, Durham University)	IIA0005
9	Name withheld	IIA0013
10	Microsoft	IIA0010
11	Wright, David (CEO, SWGfL)	IIA0008

List of Reports from the Committee during the current Parliament

All publications from the Committee are available on the publications page of the Committee's website.

Session 2024–25

Number	Title	Reference
3rd	The rights of older people	HC 414
2nd	Equality at work: Miscarriage and bereavement leave	HC 335
1st	Women's reproductive health conditions	HC 337