

## Written evidence from Microsoft [IIA0010]

**Re: Non-consensual intimate image abuse**

Dear Ms. Owen:

I write in response to your correspondence of 3 December 2024 regarding my testimony to the Committee on 6 November at its session on non-consensual intimate image (NCII) abuse. Thank you again for the opportunity to appear and for the thoughtful questions posed by the Committee.

As you and the Committee are aware, NCII content is treated differently than child sexual abuse material (CSAM) under UK law, reflecting the different practical and policy challenges in addressing each harm. In my testimony, I urged Parliament to address both the law and these practicalities. Allow me to address each in turn.

### **Legal Distinctions**

The Protection of Children Act<sup>1</sup> describes the following as illegal activity:

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

Importantly, the acts of creation and possession have been criminalized, as well as the distribution of this abhorrent content.

In contrast, the amendments to UK criminal law codified in the Online Safety Act (2023) (“OSA”) relate to the acts of *sharing*, and *threatening to share*, meaning NCII currently can be created or possessed legally in the UK, if not communicated or conveyed. The recent introduction of HL Bill 26,<sup>2</sup> which would make the act of creating or soliciting the creation of NCII an offence codified in the Sexual Offences Act 2003, is an acknowledgement of the current state of the law. As you have heard from Microsoft, we support efforts to modernize the UK’s criminal law to help deter and respond to the risk that generative AI is misused to create synthetic NCII, given the very real harms to victim/survivors.

### **Provider Obligations under OSA**

---

<sup>1</sup> Section 1(a)-(d) Protection of Children Act (1978), as amended by the Sexual Offences Act 2003.

<sup>2</sup> [Non-Consensual Sexually Explicit Images and Videos \(Offences\) Bill \[HL\]: HL Bill 26 of 2024–25 - House of Lords Library](#)

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<sup>3</sup> to have systems and processes in place to limit illegal behaviors 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. Similarly, under the current criminal law regime, the creation of NCII through generative AI features of regulated pornography services, would not appear to be covered under OSA.

Ofcom is currently developing draft *voluntary* guidelines on addressing violence against women and girls, which could provide recommendations for tackling these risks.

## **Practicalities**

It is important to note there are practical and policy differences between CSAM and NCII of adults<sup>4</sup> when it comes to detection and moderation by regulated services, whether under the OSA or through voluntary measures. In most cases, a trained content moderator can identify whether an image is likely CSAM on the face of the image alone. This is not the case in many NCII scenarios, given the key element is the question of whether or not the content has been created or shared without the consent of the person depicted. Identifying NCII requires knowledge that the content’s distribution was non-consensual. Absent, for example, visual evidence of surreptitious filming, this knowledge cannot be determined from the content alone. Without this knowledge, NCII may have the same characteristics as pornography, which is both lawful in the UK and may be permitted on many online services. The need for information about consent limits the ability for online services to apply proactive detection measures and means victims often bear the burden of notifying providers of both the content and their lack of consent. Unlike CSAM, where multiple databases are available with hashes of previously identified content, user reporting has historically been the predominant method to address the sharing of NCII.

---

<sup>3</sup> Regulated services include user-to-user services (“U2U”), search services, and pornography services.

<sup>4</sup> We note that NCII of children is likely CSAM.

Microsoft's partner, StopNCII.org, provides a partial solution to this challenge by offering victims a common reporting platform, where hashes of their imagery can be made available for use by multiple participating online services. We have advocated for government to support initiatives like this to make it easier for victims to report, and easier for providers to identify and prevent NCII from being shared.

I hope this information helps clarify the record, and deeply appreciate the care taken to address this grave societal challenge.

*December 2024*