Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 706 7329
www.microsoft.com

Microsoft

10 April 2024

To the Rt Hon Caroline Nokes MP,

Thank you for your letter dated 28 March 2024 and your interest in our approach to tackling non-consensual intimate image abuse (NCII) online. As you note, this is a horrific form of abuse and one with significant impacts for the victims, who are often women and girls. We closely follow industry and expert discussions on this topic to maintain an up-to-date understanding of the harm, including to understand the impact on victims, tactics for abuse, and best practices for addressing NCII. This is especially critical to understand the way in which emerging technology may be misused to exacerbate this harm.

Microsoft's policy prohibits the sharing or creation of sexually intimate images of someone without their permission. This includes photorealistic NCII content that was created or altered using technology. We also do not allow NCII to be distributed on our services, nor do we allow any content that praises, supports, or requests NCII. Additionally, Microsoft does not allow any threats to share or publish NCII—also called intimate extortion. This includes asking for or threatening a person to get money, images, or other value things in exchange for not making the NCII public. We have a central portal to enable victims to report any instances of their imagery to us and have for several years provided voluntary transparency reporting about our approach. We will remove NCII from our hosted consumer services and remove reported imagery from Bing's search index, helping to reduce the impact to victims. We welcome any feedback on these policies, including the extent to which they are effectively addressing the concerns about NCII that you and Committee members have heard from your constituents.

Your letter also references LinkedIn, as a major online platform where the non-consensual dissemination of intimate imagery may have particularly significant consequences for a victim, given LinkedIn's core function as a professional network. LinkedIn's Professional Community Policies reflect this purpose, including by prohibiting material depicting nudity or sexual activity. To maintain a safe and trusted experience and keep violative content off its platform, LinkedIn takes a multidimensional approach to protecting its ecosystem, including the use of artificial intelligence (AI) to help proactively filter out inappropriate content. Because nudity is prohibited on LinkedIn, AI tools are used to help detect any instances of such content (regardless of its origin). As cited in its most recent Transparency Report, LinkedIn has also enhanced its adult image detection defences in private messaging to proactively prevent the sharing of nude imagery and sexually explicit content.

However, we know that a platform-by-platform approach to NCII creates challenges for victims in effectively tackling the spread of their imagery and that the misuse of technology means this harm will continue to evolve. To address this harm effectively will require collaboration and a multistakeholder approach, leveraging the respective strengths of industry, civil society, and government.

This is why we were pleased to support StopNCII to host a meeting on this issue at our offices in New York in March 2024, at a time when critical stakeholders were gathered for the 68th session of the Commission on the

Microsoft Corporation is an equal opportunity employer.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel +1 (425) 706-4308
Fax +1 (425) 706-7329
www.microsoft.com

Status of Women. We recognize the value in bringing stakeholders together, as well as the impetus for industry to continue to evolve and improve our approaches. We also licensed a new form of PhotoDNA hash-matching technology to StopNCII and donated to support its integration, enabling victims to report their images to StopNCII without those images needing to leave their device. Because PhotoDNA hashes are already very widely used across the technology industry as a part of the fight against child sexual exploitation and abuse, offering the PhotoDNA hash format will hopefully enable a wider range of companies, including smaller companies, to join this initiative.

As Microsoft, we are also continuing our conversations with StopNCII about ways in which we can deepen our engagement and partnership, enabling us to effectively implement our policies while maintaining a risk-based and proportionate approach to safety across our diverse services. We hope to be able to provide a public update on those conversations in the coming months. We are not aware of any UK legislation that would inhibit companies from participating in a new hash-sharing initiative, but as with any new safety intervention, we need to work through a range of considerations based on the nature of the service, including assessing personal data processing and other privacy interests.

We have welcomed the recent passage of the UK's Online Safety Act and the thoughtful, evidence-based approach Ofcom is taking to its implementation. As a company with a range of services that will fall within the scope of the Act, we have been engaged regularly with Ofcom – both in the context of establishing their supervision regime and on the development of the codes of practice, guidance, and other materials critical to support compliance with the Act. While the regime will take some time to stand up, we expect the Online Safety Act will drive significant changes for business operating in the UK, including supporting a risk-based and proportionate approach to addressing a wide range of significant online harms.

The UK, unlike many other jurisdictions, has effectively criminalized the sharing of NCII, as well as the sharing of non-consensual deepfake pornography. We welcome this step and encourage lawmakers to consider whether additional measures may be appropriate to address the challenge of online services where the business model is predicated on the generation of deepfake pornography of real individuals. We also encourage law enforcement to consider bringing cases where possible, to help send a deterrent message to potential offenders.

We look forward to continuing to engage with critical UK stakeholders on this topic and, more generally, on measures to address the ongoing, global challenge of online harm against women and girls.

Yours sincerely,

Courtney Gregoire

Chief Digital Safety Officer
Microsoft Corporation