55 Almaden Blvd, Suite 600,
San Jose, CA 95113

zoom.com
1.888.799.9666

04 April 2024

To
Rt Hon Caroline Nokes MP
Women and Equalities Committee
Houses of Parliament
London SW1A OAA
United Kingdom

Re: Tackling non-consensual intimate image abuse

Dear Ms Nokes,

Thank you for your letter to our CEO Eric Yuan dated 28 March 2024 regarding non-consensual intimate image abuse ("NCII"). As the Global Head of Zoom's Trust & Safety Team, I am pleased to respond on behalf of our company.

Firstly, on behalf of Zoom, let me be clear: NCII has no place on our platform and clearly violates our Terms of Service and Acceptable Use Guidelines. It is in that spirit that we absolutely recognise the concerns you raise, and the important role technology plays in both enabling and preventing online abuse.

Zoom takes a 'Safety by Design' approach to building our products, a key part of which can be seen in how we encourage and make it straightforward for users to report content and activities that potentially contravene our Terms of Service and Acceptable Use Guidelines. These user reports are reviewed by an expert international team and can lead to action up to and including us suspending offending accounts. Our rules are clear: Sensitive content and hateful conduct are prohibited on Zoom and the sharing of non-consensual intimate images falls into both categories.

I recognise that you are principally interested in how platforms can proactively combat certain types of "revenge porn,". We agree that hashing technology is a powerful tool for companies like Zoom to fight certain forms of content proactively, as well as assist in responding reactively to user reports. For example, we work closely with the National Center for Missing and Exploited Children (NCMEC), whom you will be aware compiles the leading hashing database to help platforms including Zoom identify and remove child sexual exploitation and abuse material (CSEA) at scale. Zoom permanently suspends accounts that we determine have transmitted, displayed, stored, shared, or promoted CSEA on our platform, and we alert NCMEC, law enforcement and other entities as required by law.

55 Almaden Blvd, Suite 600,
San Jose, CA 95113

zoom.com
1.888.799.9666

I want to thank you for bringing to my attention the work of StopNCII.org. Over the past two years, we have met privately with Stop NCII and attended their roundtable in New York City. We admire the group's important work in combating NCII, and have considered implementing its technology. At present, however, we have decided to focus our resources on using hashing technology to combat CSEA material. Our decision, while difficult, was risk-based, and reflects in part the differences between Zoom and social media platforms. As a unified communications platform, Zoom facilitates real-time interactions and collaboration. Zoom does not support public user-generated content, such as text feeds or posts. Zoom users cannot follow each other or search for unknown contacts on the platform and persistent content is limited. Using our "Safety by Design" risk assessment methodology, we determined that our platform does not share the same risk of NCII as social media platforms. Indeed, our experience has shown that we do not receive a significant number of user reports related to NCII. We are confident that when material is reported by users, we are able to take swift action for it to be taken down.

Given the unspeakable harm that all forms of online abuse can cause, it is always a fraught decision how to apply limited resources. But given the above considerations, we have decided currently to prioritize our fight against CSEA. Nonetheless, we continue to track Stop NCII's work and will reconsider our decision as our efforts and the technology to combat all forms of abuse evolves.

Your letter also requested clarity on the engagements we have had with Ofcom over several years in preparation for the new Online Safety Act regime, which we have long supported. Although those conversations have never specifically focused on this type of content, we have welcomed the opportunity to deliver two workshops on Zoom's 'Safety by Design' approach for Ofcom staff and wider Government officials across the Civil Service to share our perspective and to help inform the design of the new regime.

Let me reiterate again that Zoom works hard to ensure that our users feel protected and empowered on our platform. There is no place for exploitative material here, and we will continue to implement new strategies to combat it and continue our dialogue with STOPNCII. We would be happy to meet with you and the Committee to discuss any of this in further detail.

Yours Sincerely,

Josh Parecki

Chief Compliance Officer & Head of Trust and Safety