Home Secretary and international partners tell tech companies to put child safety first

Seven countries, whose populations represent a fifth of Facebook's users across the world, have today (Sunday 11 October 2020) published an international statement on the impact of end-to-end encryption policies which erode the public's safety online.

A year after the Home Secretary wrote an <u>open letter to Facebook's Mark Zuckerberg</u> requesting the company halts its end-to-end encryption plans unless they can address child safety fears, the UK, alongside the United States, Australia, New Zealand, Canada, India and Japan, have called on all tech companies to ensure they do not blind themselves to illegal activity on their platforms, including child abuse images.

Home Secretary Priti Patel said:

We owe it to all of our citizens, especially our children, to ensure their safety by continuing to unmask sexual predators and terrorists operating online.

It is essential that tech companies do not turn a blind eye to this problem and hamper their, as well as law enforcement's, ability to tackle these sickening criminal acts.

Our countries urge all tech companies to work with us to find a solution that puts the public's safety first.

The 7 signatories of the international statement have made it clear that when end-to-end encryption is applied with no access to content, it severely undermines the ability of companies to take action against illegal activity on their own platforms.

It also prevents law enforcement investigating and prosecuting the most serious crimes being committed on these services such as online child sexual abuse, grooming and terrorist content.

This international intervention calls on tech companies to ensure there is no reduction in user safety when designing their encrypted services; to enable law enforcement access to content where it is necessary and proportionate; and work with governments to facilitate this.

The UK and its international partners are clear that they support strong encryption, but not where it is applied in a way that precludes all legal access to content, therefore putting the public at significant risk of harm.