Statement on End-to-End Encryption

The Virtual Global Taskforce is an international alliance of 15 dedicated law enforcement agencies working alongside Affiliate members from private industry and non-governmental organisations to tackle the threat of child sexual abuse (CSA).

The VGT first issued its first position statement on end-to-end encryption (E2EE) in 2021. This statement highlighted the devastating impact E2EE can have on law enforcement’s ability to identify, pursue and prosecute offenders, when implemented in a way that affects the detection of CSA on industry platforms. It is important to update the VGT position on E2EE in the context of impending design choices by industry.

As outlined in our previous statement, there is no doubt that encryption plays an important role in safeguarding privacy, however this must be balanced with the importance of safeguarding children online.

The scale of online CSA is increasing worldwide. The WeProtect Global Alliance have identified it as one of the most urgent and defining issues of our generation. The number of reports of CSA from industry continue to be staggering, but demonstrates the key role that industry plays both in protecting children online and in reporting cases to law enforcement for action.

The National Center for Missing and Exploited Children (NCMEC) received 29.3 million reports of suspected CSA in 2021, a 35% increase from 2020. Of this 29.3 million, over 29.1 million reports came from electronic service providers.
Although these reports result in a range of different outcomes globally, what is consistent is that they **significantly contribute to positive outcomes for child safety**. These figures demonstrate the current success of industry partners in detecting and reporting CSA occurring on their platforms, resulting in victims being identified and safeguarded.

Design and investment choices implemented in a way that interferes with the effectiveness of such safety systems threaten to **undermine these successes** which have been consistently built upon over previous decades. The announced implementation of E2EE on META platforms Instagram and Facebook is an example of a **purposeful design choice** that degrades safety systems and weakens the ability to keep child users safe.

META is currently the leading reporter of detected child sexual abuse to NCMEC. The VGT has **not yet seen any indication** from META that any new safety systems implemented post-E2EE will effectively match or improve their current detection methods.

By way of an example of the impact E2EE implementation could have, the following case from the United Kingdom **would not have been possible** without Facebook having access to message content, an ability they will **lose** under E2EE.

David Wilson is one of the most prolific child sexual abuse offenders the UK’s National Crime Agency has ever investigated. Wilson used META (Facebook) to contact thousands of children, grooming hundreds of victims using fake online profiles. By pretending to be a teenage girl, he manipulated victims to send sexually explicit material of themselves and in some cases, blackmailed victims into abusing their siblings and friends. Some victims were so traumatised they spoke of wanting to end their own lives.
The successful prosecution of Wilson and the resulting safeguarding of hundreds of children was possible because law enforcement were able to access the evidence contained within over 250,000 messages through Facebook. In an E2EE environment, it is highly unlikely this case would have been detected.

The VGT calls for all industry partners to fully appreciate the impact of implementing system design decisions that result in blindfolding themselves to CSA occurring on their platforms, or reduces their capacity to identify CSA and keep children safe. It is time to confront these concerns and make tangible steps towards possible solutions that we know exist.

The VGT encourages industry to respond and consider the following: Only to implement platform design choices, including E2EE, at scale alongside robust safety systems that maintain or increase child safety.

Where the child user base and risk is high, a proportionate investment and implementation of technically feasible safety solutions is paramount. The abuse will not stop just because companies decide to stop looking.

We all have a role to play in protecting children in online spaces and we strongly urge industry partners to take active steps toward this goal.