Home Office

To:
- 1: Security Minister & Safeguarding Minister (in parallel)
- 2: Home Secretary

From: Name Redacted
Tackling Exploitation and Abuse Unit, I&S
SCS: Christian Papaleontiou, Deputy Director, TEAU
Date: 3 April 2020

Tech industry response to Covid19 and online child sexual exploitation and abuse

Issue: Analysis of how Covid19 restrictions are impacting tech companies' ability to combat online child sexual exploitation and abuse (CSEA), and potential steps to improve the industry response.

Timing: Routine

Recommendations
- Agree to the steps at **para 10** to maintain pressure on industry to combat online CSEA (including more complex cases) during the Covid19 period and encourage collaboration.
- Note that lockdown guidance does not specifically prevent companies from having moderators attend the office, where these roles cannot be carried out at home - **para 3**
- Note industry's offer to contribute to comms and preventative messaging (advice to follow once these plans have been further developed) - **para 12**
- Agree to point parents towards tools to manage younger children's use of online platforms (rather than focussing on the dangers of underage children using social media) – **para 13**
- Agree to write to companies (jointly with other Five Eyes Ministers) to reiterate the importance of this issue, highlighting the NCA's threat assessment and encouraging collaboration – **Annex A**
- Note more specific and potentially controversial requests that could be made, if we have more evidence to justify it – **para 14 and 15**

Devolution implications: N/A

Has the use of analysis/ evidence/ data/ statistical information in this submission been agreed by Home Office Analysis and Insight? N/A

Has the scientific information in this submission been agreed by Home Office Science? N/A

Has a Policy Equality Statement been completed? N/A

Has the central Home Office finance team been consulted? N/A

Has relevant legal advice been received? N/A

Discussion

Assessment of industry response to Covid19

1. **With medium to high confidence, it is highly likely that COVID-19 will increase the risk of online child sexual exploitation and abuse (CSEA).** This is due to the combination of increased volumes of children online, child sex offenders likely with more time available seeking to exploit this and reduced capacity of company moderators and NGOs. Risks could include offenders having more time to share imagery with each other, children at increased risk of grooming and being coerced into self-generating indecent imagery on social media, gaming and livestreaming platforms, and offenders commissioning more livestreamed abuse.

2. **Tech companies' ability to combat this activity is reduced, due to having fewer human moderators.** Whilst most CSEA is detected using automated tools, companies rely on human moderators to verify the results of the tools, and take action such as closing accounts, carrying out further investigation, and assembling quality reports for law enforcement. Some companies' moderators continue to work but with reduced capacity due to social distancing requirements and illness, others are working from home where it is difficult, for welfare reasons, for staff to view child abuse material.

3. **Current UK guidance does not specifically prevent moderators from continuing to travel to work, should this be necessary due to the viewing of child abuse material. It states:** *"You may travel for work purposes, but only where you cannot work from home."* However whilst some moderators work in the UK, many do not, and are following local guidance.

4. **To address the shortfall of moderators, companies are having to prioritise and changing their use of automated tools.** Most companies state they are prioritising CSEA, along with terrorist content and Covid19 response. However, early information from NCMEC (the US NGO where companies are required to report instances of CSEA) is that whilst straightforward cases of known imagery that can be referred using automated methods continue to be reported, reporting of more complex CSEA cases requiring human investigation (for example, grooming or offenders contacting multiple victims) is dropping off.

5. **Increased reliance on automated methods is an option for some parts of the CSEA threat** (for example known imagery, where accuracy rates are high) but not others (eg grooming, where the greater need for human context means it is unlikely companies can fully automate the process). Where companies are turning to fully automated methods, some are adjusting the tools' accuracy thresholds to reduce false positives (which is important for law enforcement too, to avoid being overwhelmed by reports) but this comes at a trade off of more CSEA content passing through undetected.

6. **Other safety measures remain unchanged.** Companies already implement a range of safety measures and some limited educational materials and preventative messaging. There are no indications that companies intend to step up existing safety approaches; however some are considering additional

educational/preventative approaches and have agreed to work with Government and law enforcement on this.

7. **NGOs ability to support the system is also reduced**. NCMEC are unable to view child abuse imagery with staff working from home, so are no longer able to analyse and fully triage CSEA referrals from industry to assist law enforcement. This responsibility has now been taken on by the NCA to minimise impact on UK law enforcement. The Internet Watch Foundation are operating at 50% capacity in order to maintain distancing between workers. Following their meeting with Home Office Ministers last week, they have reviewed their decision to focus on public reports and will now be directing 80% of analyst time to proactively identifying content (which is more efficient, as the accuracy rate is much higher) and 20% to dealing with public reports. This will lead to a slower response time to public reports, but they will communicate the potential delay to people reporting. IWF also report other hotlines and smaller websites being unable to respond and remove this material at the usual rate.

8. **We will continue to work with law enforcement, NGOs and companies to improve and update this assessment and identify any new risks.**

<u>Options to improve the response</u>

9. **We recommend pursing options 1-3 now, and keeping 4-5 on hold until we see how the threat and industry response manifests in practice.**

10. **Option 1: maintain pressure on industry to combat CSEA (including more complex cases) during the Covid19 period, keep companies informed about specific risks and encourage collaboration.** This option is recommended at this stage as it allows companies to use their own expertise to identify the best way to address the problem. More specific requests risk being infeasible or having unintended consequences unless fully investigated. We could achieve this by:
    a. Continuing to engage Five Eyes Governments on Covid19 risks and company response; by companies' own admission this international approach raises pressure on them. Legal issues mean the US Government cannot direct companies but, following discussions yesterday, we now have agreement from all 5 countries to engage industry as a collective.
    b. Sharing threat assessments, screen shots of offender chat and evidence from NGOs, to ensure companies are aware of the risks and the intent of offenders to exploit their platforms and reductions in human moderators.
    c. Encouraging companies to collaborate and share information with each other and Governments; companies are reluctant to do this (possibly due to concerns around a public message that CSEA offenders operate on their platforms) but we believe we now have agreement on the terms of a discussion between Five Eyes and six of the main tech companies.
    d. Clear Government message that more complex threat elements such as grooming, livestreaming and new imagery (as set out in the Five Eyes voluntary principles for industry) should continue to be addressed, even though they consume more human resource, because they often indicate a new victim and therefore more immediate risk.

e. Asking NCA to develop company specific intelligence, where vulnerabilities relating to a particular platform are identified. This is challenging for NCA but will allow companies to seek ways to close the vulnerability.
f. To support the above, we recommend you (James Brokenshire) write to companies, highlighting the NCA's latest Covid19/CSEA threat assessment and reiterating the importance of a collaborative response. Other Five Eyes have indicated willingness to sign this letter which would carry more weight (other work can continue whilst we complete sign offs). We will circulate the draft at **Annex A** to other countries and return for your final signature.
g. As a last resort, making information about specific problems public has been shown in the past to prompt urgent action from companies.

11. **Alongside this, we will continue to drive long term progress against the Five Eyes voluntary principles for industry, including by:**
a. Continuing to work with the We Protect Global Alliance to develop their plans to promote the principles more widely and understand their implementation.
b. Supplementing this with our own VTC bilaterals with European countries, to broaden the reach beyond Five Eyes Governments.
c. Fortnightly calls with Five Eyes partners to share information on the threat, particular platform vulnerabilities, and emerging policy areas such as safety measures for encrypted platforms.
d. Work with NCA, GCHQ and undercover online officers to develop new capability to use intelligence to highlight where companies are not implementing the principles effectively.
e. Work with NGOs to encourage them to make their own assessments of where individual companies are not complying or collectively need to do more.
f. Developing the UK Code of Practice as a source of more detailed guidance on how the principles can be implemented. The Code will also form part of future online harms regulation in the UK.

12. **Option 2: comms and preventative messaging.** Following initial discussions with Five Eyes and companies, companies have indicated they will work with us to develop a safety campaign on CSEA for parents and children. Companies could support and amplify Government, law enforcement or charity comms/educational materials (for example, through targeted advertising to parents). They could also highlight their own safety controls and advice through messaging and 'nudges' to users (including children), particularly new users or those whose usage pattern has changed. We will work closely with NCA, charities, DCMS, DfE to develop this with companies and provide further advice.

13. **Option 3: addressing underage users**. A significant number of grooming victims are children aged U13 and below the age limit of the platforms they are groomed on. To reduce this risk to younger age groups, we could ask companies (and parents) to step up their vigilance on underage accounts. An alternative proposal, accepting that many parents will allow underage children access, is to promote the use of safety tools which allow parents to control settings (for example, limit who a child can contact) or analyse content and send warnings to parents about potentially harmful interactions. Government could raise awareness of these tools in our own comms or ask tech companies to do so. We would need to consider how directive a message is given. Parental tools would