The Virtual Global Taskforce (VGT), an international collaboration of law enforcement agencies, NGOs and industry partners, has the sole objective to protect children from online sexual exploitation and transnational sex offences. Its strategic goals include supporting the private sector to improve its protective security by sharing intelligence on the threat to children from online sexual exploitation and abuse. As such, we have followed with interest the developments in Europe regarding the introduction of legislation to preserve the ability of electronic communications networks and services to detect child sexual abuse and exploitation material and grooming behaviour on their platforms.

It is important to emphasise that the priority of law enforcement globally, including those that are members of the VGT, is always sharply focused on the victims of this crime. Those victims suffer not only from the actual physical effects of sexual abuse per se but also, repeatedly through the creation, distribution and circulation of child sexual exploitation materials (including images, videos, and written words) of their abuse. Many victims have stated that the continued circulation of their sexual abuse has debilitating and humiliating consequences for them, which continue throughout their adult lives. Locating victims so that they can be removed from harm, and being able to prevent the re-circulation of child sexual exploitation materials (CSEM), are positive steps for service providers toward preventing re-victimisation at various levels. Further, preventing children from becoming victims by detecting language patterns that indicate they are being groomed or solicited for the sharing of CSEM is also welcomed since it enables the detection of offending behaviour while preventing it from becoming hands on sexual exploitation, at least in some cases. Finally, preventing children from being forced into producing additional CSEM through the re-circulation of self-produced images, protecting them from the associated emotional turmoil and trauma is a constructive use of technology. The VGT is familiar with the technologies used to achieve these aims and the effect on victims of the re-circulation of CSEM through its private sector partners who implement them in their systems and our NGO partners efforts in working with those most affected by this crime.

The VGT is also familiar with the effect that preventing the use of those technologies will have on the ability of law enforcement agencies to counter the crime of online child sexual exploitation. That effect will be quite profound. In 2019, the US based National Centre for Missing and Exploited Children (NCMEC) CyberTipline received more than 16.9 million reports from electronic service providers, most of which related to: apparent child sexual abuse material; online enticement, including "sextortion"; child sex trafficking and child sexual molestation. NCMEC estimates that the number of CyberTips currently generated by proactive checking of private messaging for CSEM would be reduced by up to 70% if measures are implemented to prevent that. This means that 7 out of 10 of those investigations that law enforcement are currently able to pursue based on these would not be possible. In those cases, offenders who are grooming children in preparation for child sexual exploitation and abuse will not be located and will continue to endanger children. Additionally, the likelihood of being able to link offenders to material that they have been involved in circulating through one-to-one messaging online, will be reduced by approximately 70%. To illustrate what this means at a country level, in the year ending June 2020, the UK's National Crime Agency made over 15,734 disseminations to police forces

from industry referrals. In the same year, industry reporting led to UK law enforcement arresting over 4,500 offenders and approximately 6,000 children being safeguarded.

For clarity industry referrals to law enforcement are based on findings from victim reporting, artificial intelligence and human moderation. Industry is careful to preserve the privacy of its users, with almost all using AI to flag concerning behaviours which can be detected without viewing user generated content. Human moderation is generally only deployed in public areas of social media platforms following a report from a user who is a victim or witness to child sexual abuse, or following AI indicators which meet a high threshold for human moderation.

Industry's proactive prevention methods include use of software and hash lists to identify known CSEM to prevent offenders from uploading material that has already been identified as criminal. They can carry out this work without seeing the content of users' communication in a similar way to how anti-virus software is deployed. Some companies also use URL block lists to prevent users from purposefully or accidentally accessing CSEM and they work closely with international hotlines to support companies to remove this illegal content from their domains and infrastructure. Overall, the steps industry takes are carefully balanced with the need to protect users privacy whilst also prioritising the safeguarding of children.

At this point the legislators in the European Parliament are contemplating how to legislate in this matter. As a network of law enforcement agencies we urge all of those involved to consider strongly the right to privacy of the victims directly affected by this crime, while also taking account the consequences for society of drastically reducing the ability of law enforcement to investigate breaches of those rights.

Thank you for your consideration.
Chief Superintendent Marie-Claude Arsenault, Royal Canadian Mounted Police
VGT Chair