VGT position on End-to-End Encryption

The Virtual Global Taskforce (VGT), an international alliance of law enforcement agencies, comprised a law enforcement board of management (BoM). The VGT BoM works with key non-governmental organizations (NGOs) and industry partners. Its mandate is to protect children from online sexual exploitation and other transnational child sex offences. One of 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 with regard to End-to-end encryption (E2EE), the use of encryption technologies, and their effects on the ability to detect child sexual exploitation material (CSEM) and grooming behaviours on social media and messaging platforms.

The priority of law enforcement globally, including members of the VGT, is on the victims of online child sexual exploitation. Victims suffer not only from the actual physical effects of sexual abuse but also ongoing victimization through the production and distribution of CSEM. Many victims have stated that the continued circulation of their sexual abuse has negative consequences for them often throughout their adult lives. Locating victims so that they can be removed from harm, and the ability to prevent the re-circulation of CSEM, are positive ways in which service providers can help to prevent re-victimization at various levels. Industry efforts toward preventing children from becoming victims by detecting language patterns that indicate grooming or solicitation for the sharing of CSEM are also supported. These efforts also have the potential of preventing hands on sexual abuse.

The VGT is aware of the negative effect that E2EE has on the ability of companies and law enforcement agencies to counter the crime of online child sexual exploitation. In 2020, the US based National Centre for Missing and Exploited Children (NCMEC) CyberTipline received more than 21.4 million reports from electronic service providers, most of which related to: apparent CSEM; online enticement, including “sextortion”; child sex trafficking and child sexual molestation, 20.3 million of these reports were from Facebook. In 2018, Facebook Messenger was responsible for 12 million of the 18.4 million reports of CSEM to NCMEC. The WePROTECT Global Alliance assessed in 2019 that these reports risk disappearing if E2EE is implemented, since current tools used to detect online child sexual exploitation do not work in end-to-end encrypted environments. In the same year, NCMEC also released a statement saying that “if end-to-end encryption is implemented without a plan/solution to safeguard children, NCMEC estimates that more than half of its CyberTipline reports will vanish”.

For clarity, industry referrals to law enforcement are based on findings from victim reporting, artificial intelligence (AI) 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 the 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 taken by industry are carefully balanced with the need to protect user privacy while also prioritizing child protection.

Some Internet Services Providers, application developers and device manufacturers are developing and deploying products and services with E2EE. The effect of this is to prevent them from detecting the sexual exploitation of children occurring on their platforms, as well as preventing them referring such detections to law enforcement for investigation including serving them legal warrants in order to identify offenders and victims. E2EE, is designed to prevent industry partners and others from accessing user content, requiring them to rely on AI to detect behavioural indicators through metadata. While much can be deduced from metadata, it is usually insufficient to meet the threshold required for a search warrant. Furthermore, the companies themselves advise that oftentimes individuals identified through these methods only meet their policy threshold for warnings or exclusion from some features on the platform, and do not trigger a report to law enforcement. Ultimately, E2EE creates a risk that companies are unable to adequately safeguard children using their services since they do not have enough information regarding online behaviours to warrant sharing referrals on potential abuse with law enforcement. Protecting those victims whose abuse has already been recorded and could be circulated through services where E2EE is used is also made much more difficult.

The VGT urges all of those involved to consider strongly the right to privacy of the victims directly affected by this crime, while also taking into account the consequences for society of drastically reducing the ability of law enforcement to investigate breaches of those rights and remove children from harm. We also support the Five Eyes statement and encourage technology companies to work with governments to take the following steps, focused on reasonable, technically feasible solutions:

- Embed the safety of the public in system designs, thereby enabling companies to act against illegal content and activity effectively with no reduction to safety, and facilitating the investigation and persecution of offences and safeguarding the vulnerable;
- Enable law enforcement access to content in a readable and usable format where an authorization is lawfully issued, is necessary and proportionate, and is subject to strong safeguards and oversight; and,
- Engage in consultation with governments and other stakeholders to facilitate legal access in a way that is substantive and genuinely influences design decisions.

Thank you for your consideration.

Chief Superintendent Marie-Claude Arsenault, Royal Canadian Mounted Police
VGT Chair