Google Australia Pty Ltd
Level 5, 48 Pirrama Road
Pyrmont, NSW 2009
Australia

google.com

20 August 2021

Parliamentary Joint Committee on Law Enforcement
PO Box 6100
Parliament House
Canberra ACT 2600

BY EMAIL: le.committee@aph.gov.au

Dear Committee Members,

Google welcomes the opportunity to provide feedback to the Committee on the inquiry into law enforcement capabilities in relation to child exploitation.

Now 22 years old, Google has grown from a small start-up to a global company with legal obligations in each of the countries in which we operate. We work hard to protect our platforms from abuse and have been working on this challenge for years, using both computer science tools and human reviewers to identify and stop a range of online abuse, from the "get rich quick" schemes and disinformation, to the utterly abhorrent, including child sexual abuse material (CSAM).

Our Terms of Service prohibit the use of Google's platforms or services to exploit, abuse or endanger children and we respond promptly to notices from third parties and users regarding any such content. We recently published the first of what will be a twice-yearly transparency report that details Google's efforts and resources to combat CSAM across our platforms.

A mix of people and technology help us identify potentially violative content and enforce our policies, and we continue to develop and invest in smart technology to detect problematic content hosted on our platforms, which is driving tangible progress.

We also work closely with peer companies across the industry through our collective investment in the Technology Coalition. We know that no one company or platform can do it alone when it comes to protecting children. That is why Google has significantly contributed to the Technology Coalition, building shared knowledge, funding research and developing cutting edge technology and coming together with others - government, educators, parents, law enforcement - to protect children on our platforms and across the Internet.

Google offers a broad range of consumer and enterprise products and services in Australia, including our Search engine, YouTube video sharing platform, Gmail, Google Maps, the Android mobile operating system, Google Play Store marketplace, the Chrome web browser, Google Photos, the Drive file storage and sharing application, home speakers and smart devices such as smoke alarms, and more.

The common thread that runs through all of these products is that they are designed with the safety and security of our users foremost in our mind. We are proud to have contributed to the development of the eSafety Commissioner's Safety by Design Principles and we publicly support them.

We will focus our contributions to items 4 and 5 from the inquiry terms of reference.

Encryption

Encryption is a critically important tool in protecting individuals, corporations, governments and agencies from a broad range of security threats, including the interception and misuse of personal, financial or national security information. We design our products and services with advanced security at their core -- from our custom-built infrastructure that protects our data centres and servers to layers of advanced encryption that protect user data. Various forms of encryption are used across Google's consumer and enterprise products, such as Android, Chrome, Meet, Gmail, and Cloud and forms a key part of the security assurances we provide to users and customers.

For business customers, encryption may be necessary to comply with applicable laws and regulations or industry-specific standards, so we build our products to support those requirements. For example, the Australian Privacy Principles (APPs) require entities that hold personal information to take steps to "protect the information from misuse, interference and loss; and from unauthorised access, modification or disclosure".[1] The Office of the Australian Information Commissioner's Data Breach Preparation Guidelines also refer to the benefits of encryption.

End to end encryption (E2EE) has become the industry standard for real time communications and it's what Internet users have come to expect. Google has begun a phased roll out of E2EE for one-to-one conversations solely between Android Messages users.

[1] See APP 11.1.

We are mindful of the risks that encrypted communications can be misused and abused by bad actors to facilitate the sharing of CSAM. We believe that there are appropriate tools to fight the spread of CSAM even in encrypted environments. Those tools include using behavioural information and meta-data signals, which can be deployed to detect behaviours that may be putting children at risk, and we are committed to working constructively on innovation in this area. Further research, refinement, and technological innovation will rely on the appropriate legal frameworks being in place in support of this mission.

Our investment in child safety protections and dedication to child safety remains steadfast and extensive across our products. In 2020, Google submitted over 540,000 reports, containing a total of over 4.4M uploaded files, to the National Centre for Missing & Exploited Children (NCMEC). NCMEC is a private, non-profit organisation established by the United States Congress to serve as the clearinghouse and reporting centre for all issues related to the prevention of and recovery from child victimisation, who act as an intermediary between the technology industry and law enforcement agencies. Where material is escalated to NCMEC that appears to have an Australian nexus, information is passed to the Australian Federal Police for further investigation.

Strong encryption doesn't create a law free zone; companies can still deploy several anti-abuse protections using metadata, behavioural data, and new detection technologies without seeing the content of messages encrypted in transit (thereby respecting user privacy). Our work to increase the cybersecurity posture of users while enabling law enforcement agencies to investigate and solve crimes demonstrates that the goals of public safety and user security are compatible.

We need to find ways to enable this work without engineering vulnerabilities into products and services in ways that weaken security for all users. There are a lot of opportunities to work together to reduce challenges confronting law enforcement regarding obtaining digital evidence. The Centre for Strategic and International Studies (CSIS) report on "low hanging fruit" remains a good and relevant resource for recommendations to improve the ability of law enforcement to obtain digital evidence.

Child Sex Abuse Material (CSAM)

Google is one of the leaders in fighting CSAM and our goal is to make sure that we are not part of the supply chain for this content. We approach this fight against CSAM by 1) developing technology to fight abuse on our platforms, and 2) working across industry and with NGOs to support the development of new data-driven tools, boost technical capacity, and raise awareness.

CSAM is illegal and we do not allow such content to be created, distributed or stored on our platforms. The accounts responsible for its creation, distribution and storage are reported to the respective authorities upon identification, and in 2020 we disabled over 175,000 accounts for possessing CSAM.

We develop and deploy cutting-edge technology to improve our own efforts to identify, remove, and block CSAM across all our platforms:

1. In 2008, we began using "hashes," or unique digital fingerprints, to identify, remove, and report copies of known images automatically, without humans having to review them again.
2. We contribute new hashes to, and receive hashes from other platforms, via a hash database maintained by the NCMEC. This database is made available to participating service providers so that content identified on one platform can be swiftly removed from all participating platforms.
3. In 2015, YouTube engineers created CSAI Match, a first-of-its-kind, world leading fingerprinting and matching technology that can be used to scan and identify uploaded videos that contain known CSAM. CSAI Match allows us to identify known CSAI content in a sea of innocent content. When a match of CSAI content is found, it is then flagged to partners to responsibly report in accordance with local laws and regulations:
a. Since this technology was publicly introduced in 2015, Google has voluntarily shared over 100,000 video hashes with industry (through NCMEC) to allow other companies to prevent the distribution of these videos on their platforms as well; and
b. We make this technology available to other platforms and NGOs free-of-charge.

4. In 2018, Google engineers created the Content Safety API which helps Google and partners identify new never seen before CSAM, at scale, which was not possible using hash matching alone:
a. The Content Safety API classifier uses programmatic access and artificial intelligence to help our partners classify and prioritise billions of images for review;
b. The higher the priority given by the classifier, the more likely the image contains abusive material, which can help partners prioritise their human review and make their own determination of the content;
c. Partners must conduct their own review in order to determine whether they should take action on the content; and
d. We make this technology available to partners free of charge.

Google regularly accepts URL lists from anti-CSAM organisations and third party organisations which further adds to the body of known CSAM that can be detected. This is another way in which Google becomes aware of CSAM and is able to take action. Organisations that are committed to child protection and online safety, such as the Internet Watch Foundation (IWF), Interpol, the NCMEC and Freiwillige Selbstkontrolle Multimedia-Diensteanbieter (FSM) regularly provide Google with lists of URLs that contain content identified by the relevant organisation as CSAM. We use these lists to detect and block URLs containing CSAM from appearing within our Search index.

Support for law enforcement agencies

Google appreciates that law enforcement agencies face significant challenges in protecting the Australian public. Google has a longstanding and well established process for responding to lawful requests from Australian law enforcement agencies to access Google account data.

In 2020, Google received 5,914 data access requests from Australian law enforcement agencies. We received a further 35 requests under our emergency disclosure policy which facilitates access to account data in urgent circumstances where life is at risk and we staff this service 24 hours a day, seven days a week, 365 days of the year - globally.

Under U.S. law, the Stored Communications Act allows Google and other service providers to voluntarily disclose user data to governmental entities in emergency circumstances where the provider has a good faith belief that disclosing the information will prevent loss of life or serious physical injury to a person.

The Clarifying Lawful Overseas Use of Data Act (CLOUD Act) is a United States federal statute enacted in March 2018 that establishes clear guidelines and procedures around lawful requests for cross-border access to data held by US based companies. The CLOUD Act enables the US Government to enter into executive agreements with qualifying foreign governments to facilitate the disclosure of communications content within a US technology provider's possession, as an alternative to working through the Mutual Legal Assistance Treaty (MLAT) process. Google encourages the Australian Government to enter into an executive agreement with the US Government as this will not only expedite lawful requests to access communications content but also improve safeguards around the production of evidence in Australian criminal proceedings.

We deliver regular training to agencies to ensure that they are aware that we can assist with investigations involving Australian residents. When we become aware of statements on our platform that constitute a threat to life or that reflect that someone's life may be in danger, we report this activity to law enforcement agencies.

Our policies for lawful data access require that we recognise the jurisdictional constraints that law enforcement agencies operate within.

Content classification on streaming services

Age restricted videos on YouTube

There is clearly a wide and diverse range of video based content available on YouTube, with more than 500 hours of content uploaded to YouTube every minute from all around the world. Content that violates YouTube's Community Guidelines is removed from YouTube's main service. However, sometimes content doesn't violate these policies but may not be appropriate for viewers under 18. In these cases, we may place an age-restriction on the video, in the manner as explained in the paragraph below.

This policy applies to videos, video descriptions, custom thumbnails, live streams, and any other YouTube product or feature. This includes, but is not limited to, violent or graphic content; content promoting a product that contains drugs, nicotine, or a controlled substance; pranks or dangerous acts that a minor could easily imitate or a video about fake harmful pranks that seems so real that viewers can't tell the difference; or content meant for adult audiences but could easily be confused with family content. Again, this is not an exhaustive list, and we provide more detailed information about what content may be eligible for age-restriction on the help centre pages for each of our content policies.

Age-restricted videos are not viewable to signed out users, users with a declared age of under 18 years or users who have "Restricted Mode" enabled[2]. Also, age-restricted videos cannot be watched on most third-party websites. Viewers who click an age-restricted video on another website, such as an embedded player, will be redirected to YouTube or YouTube Music. Once there, they can only view the content when signed in and over 18. This process helps make sure that no matter where content is discovered, if a video is hosted by YouTube it will only be viewable by the appropriate audience.

Beginning September 2020, videos are identified for age-restriction via our automated systems[3].

YouTube Kids - One of the key motivations behind developing the YouTube Kids app was to create a safer environment for children under 13 to access age appropriate content on YouTube, which we continue to recommend to parents who plan to allow their children under 13 to watch independently. Parents can approve the specific content they allow their children to watch and can control their screen time.

YouTube Originals - Since 2016, YouTube has licenced a relatively small number of shows (currently around 150) on an exclusive basis for a specific window on the platform, labelled YouTube Originals. Where this content is available to users only on a commercial basis (i.e. for a fee), we work with a third party to apply Australian classification ratings.

Movies and TV series - YouTube also offers the latest movies and shows for purchase or rent. These films carry an Australian classification rating.

Other potentially harmful content - Beyond content which accords with our Community Guidelines but may be harmful for minors, YouTube has made a significant investment over many years in technological and human resources to quickly identify and remove harmful content such as CSAM and terrorist content. We have also made a number of more recent changes, including blocking comments on videos featuring minors.

[2] Turning "Restricted Mode" on applies a filter that seeks to remove adult oriented content from YouTube search results.

[3] https://blog.youtube/news-and-events/using-technology-more-consistently-apply-age-restrictions/

We note that the Government is in the process of reviewing Australia's classification regulations and that certain responsibilities under the Classification (Publications, Films and Computer Games) Act 1995 have been conferred on the eSafety Commissioner through the recently passed Online Safety Act 2021. We have been engaging in both of these law reform processes and would be happy to answer any questions the Committee has in this regard.

Yours sincerely,

Samantha Yorke
Government Affairs and Public Policy