13 april 2021

Consultatie Wet bestuursrechtelijke aanpak online kinderpornografisch materiaal

We thank the Dutch government for the opportunity to submit feedback to the Dutch administrative law act on combating online child pornographic material (hereinafter "the Act").

We endorse the Dutch government's objective to remove child sexual abuse material (CSAM) from the internet. Google is fully committed to fighting online child sexual abuse and exploitation on our platforms, and as a member of of the Technology Coalition, we also regularly contribute to the wider fight by collaborating with others in the sector, lending our knowledge and technology to strengthen the global response to combat this very serious crime.

We see the similarities between the Act and the objectives of the European Commission as set out in the EU's strategy for a more effective fight against child sexual abuse[1], and the announced legislative proposal of the EC to "*tackle child sexual abuse online more effectively, to better protect victims' rights, and to work towards the possible creation of a European centre to prevent and counter child sexual abuse*"[2]. We look forward to expanding on ideas on this important subject with the Dutch government and also with the EC in our submission to the Commission's open public consultation.[3] It is crucial that national legislation is consistent with the wider European framework in the fight against CSAM - this is a global crime that requires a coordinated approach and a global response.

As written, the Act would not apply to Google, since its relevant entities are established outside the Netherlands. Nonetheless, we would like to take advantage of the opportunity to suggest the following guiding principles when developing the final text.

Enhancing legal certainty of applicability of the Act on communication providers

The explanatory memorandum stipulates the scope of the Act is limited to providers of communication services, referencing the subcategories from artt. 14-16 of the e-Commerce Directive: providers of (i) mere conduit, (ii) caching and (iii) hosting services. In this context, 'providers of hosting services' is a broad concept which also includes providers whose activities partly consist of hosting. According to the explanatory memorandum, the definition encompasses providers of server space like datacenters, social media platforms, video streaming services and ISPs that offer their own server space to store data like websites, images and video files.

[1] EU strategy for a more effective fight against child sexual abuse COM(2020) 607 final.
[2] EU strategy for a more effective fight against child sexual abuse COM(2020) 607 final, p. 4-5.
[3] https://ec.europa.eu/home-affairs/news/fighting-child-sexual-abuse-have-your-say_en.

The explanatory memorandum also clarifies that the Act is only applicable to providers of communications services that are established in the Netherlands, stipulating that the Act does not deviate from the 'Country-of-Origin' principle laid down in Article 3(2) E-Commerce Directive[4]. For the purpose of legal certainty, we recommend to clarify this limit in scope in the actual text of the Act as well.

Google's communication services are provided by entities not established in the Netherlands, including Google LLC established in the United States and Google Ireland Limited established in Ireland. As such, we consider the Act not to be applicable to us. Google is however fully committed to the global response to combat the presence of CSAM online. It supports the purpose of the Act, and also contributes to the fight against CSAM through its existing policies, collaborations and enforcement mechanisms. Google supports a clear, consistent and effective European legal framework to combat CSAM, and is happy to discuss this with the Dutch government in more detail.

Creating the right support for providers to continue their voluntary detection of CSAM and to encourage providers to innovate and grow without fear of unintended consequences

The current system for the detection and reporting of CSAM has created the conditions for many providers to invest, improve and innovate in the fight against this egregious content. Over the years, Google has continued to invest in technologies to help the detection of CSAM. In 2020, the National Center for Missing and Exploited Children (NCMEC) received 21.3 million reports from industry, of which 548k were from Google, the second company in terms of reports to NCMEC.

Since 2008 we have been using hash matching technology to detect known CSAM on our services. We have developed this technology to allow us to detect the hashed image even if the image has been slightly altered. We have further evolved the technology to detect videos containing known CSAM content and make it available to others in the sector free of charge through CSAI Match.

We have also developed machine learning classifiers to detect not previously identified CSAM. Classifiers allow us to keep up with bad actors by helping us identify new content likely to contain CSAM, which can then be prioritised for human review. The use of classifiers combined with human reviewers help us identify never before identified CSAM, which can lead to the rescue of children undergoing ongoing abuse, and allows us to continue to grow the corpus of known CSAM that can be further detected using hash matching technology in a virtuous circle. We make the technology underlying our classifiers available to third parties free of charge through the Content Safety API.

[4] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

All these efforts have taken place under a legal regime that does not impose specific obligations or high barriers of entry on providers to continually innovate to better detect known or unknown CSAM. The Dutch government rightly acknowledges the success of self-regulation in our sector in the fight against CSAM.

The Act obliges hosting providers to take "*appropriate and proportionate measures*" against CSAM on a best efforts basis (Article 8(1)) that can be enforced by the Authority with an order subject to a fine if a hosting provider is repeatedly confronted with CSAM and fails to take a minimum obligation of preventive measures (Article 8(3)). Under the Act, the Authority can provide instructions to make certain CSAM and material similar to that CSAM inaccessible (Article 9(1)), that can be enforced by the Authority with an order subject to a fine and/or a cease and desist order (Article 9(4) and Article 10). Notwithstanding the voluntary measures that hosting providers may implement to detect and remove CSAM content on their services, formal instructions based on the Act should be in accordance with Article 8 of the proposed Digital Services Act, and for example include sufficient information (such as a URL) to identify the content at issue. In this context, the explanatory memorandum also correctly stresses the Authority cannot oblige communication providers to generally or systematically monitor all transmitted data or uploaded content, to actively search for CSAM, nor to independently assess whether content is similar to certain CSAM that needs to be made inaccessible, which would all be contrary to Article 15 E-Commerce Directive.[5]

Article 14 of the Act states that *"The person who makes online child pornographic material inaccessible shall transfer a copy of the corresponding data to the Authority."* As a U.S. based company, Google is under an obligation to report to the National Center for Missing and Exploited Children (NCMEC) when we become aware of offenses involving CSAM on our platforms. We feel it is important to stress the importance of developing legislative requirements that build on the existing infrastructure of reporting and handling CSAM content, avoiding duplicative and inconsistent requirements. NCMEC has a well established infrastructure and over the years, NGOs, law enforcement and providers around the world have invested to make this system work. While we currently do not transmit CSAM to national authorities, NCMEC has well established secured networks in over 130 countries/territories. Using this infrastructure, in 2019 and 2020, NCMEC sent over 25k CyberTip reports to the policy in the Netherlands. In considering imposing obligations for Dutch based companies to report to the Authority, the Act should not create duplicate obligations for data transmission, and ensure these obligations fit within the upcoming reporting system that the European Commission is considering.

We understand the considerations of the Dutch government behind the need for effective administrative competences to take action against communication providers who systematically fail to take down CSAM in a timely manner. We encourage the fact that the Act does not impose general obligations on communication providers to monitor content, report CSAM to the Authority or to implement specific preventive measures, but that the Dutch government

[5] A formal instruction to remove content *similar* to certain CSAM cannot require the manual screening of content, but must be possible in an automated manner. CJEU 3 October 2019, C-18/18 (*Facebook/Glawischnig-Piecszek*), also see: District Court of The Hague 17 March 2021, ECLI:NL:RBDHA:2021:2422, par. 4.36 and further (*Facebook/PVH*).

introduces a flexible framework allowing tailored action against those communication providers who systematically fail to take action voluntarily under the current Dutch self-regulation system. It is important that the final text of the Act also does not end up unintentionally creating barriers for providers to detect and report CSAM. Proposals that impose unrealistically low error rates, transparency requirements and burdensome administrative steps can inadvertently deter companies from voluntarily detecting this content in the first place.

We believe that the fight against child sexual abuse and exploitation online requires a global response and we work across the sector and with NGOs to collaborate and share expertise for a more effective fight against this illegal content. Created in 2006, the Tech Coalition currently comprises 20 of the largests companies in the sector. The Tech Coalition recently launched Project Protect to further support industry's collaborative efforts around research, technology and innovation, information and knowledge sharing, transparency and accountability and collective action. The Tech Coalition is looking to expand its membership to other organisations with the view of strengthening the fight aganst child sexual abuse and exploitation across the sector.

Aligning the Act with EU legislation to avoid legal uncertainty for communication providers

Article 8(1) of the proposal contains a best efforts obligation for hosting providers to "*take appropriate and proportionate measures to limit the storage and the transmission of child pornographic content online through its services"*. The explanatory memorandum stresses this concerns a "best efforts" obligation and as indicated earlier, does not oblige communication providers to generally or systematically monitor all transmitted data or uploaded content, nor to actively search for CSAM.

At EU level, there are other legislative initiatives that will impose rules on hosting providers to take action on illegal content, such as the Digital Services Act (DSA)[6] and, specifically for CSAM, the previously mentioned forthcoming regulation that the European Commission is proposing. It is important that the wording and meaning of the obligation to take appropriate and proportionate measures in article 8(1) is/becomes aligned with similar obligations under these EU laws. After all, the DSA precludes that national legislators set national rules in the harmonised area. If service providers abide by their obligations to combat CSAM under the DSA and CSAM regulation, the obligation under Dutch law to take appropriate and proportionate measures must be deemed fulfilled too. For example, the DSA stipulates that there is a need to put in place "*appropriate and proportionate safeguards*" against misuse of services of online platforms by recipients of the service frequently providing manifestly illegal content[7]. In anticipation of the DSA, and in order to avoid legal uncertainty for communication providers, what will be considered as "appropriate and proportionate" under the DSA should not be different from under the Act and vice versa.

[6] Proposal of a Regulation on a Single Market For Digital Services and amending Directive 2000/31/EC (E-Commerce Directive) (COM(2020) 825 final).
[7] Recital 47.

When the EC presents its legislative proposal to combat online child sexual abuse, we encourage the government to adjust the Act to this new legislation, by specificially adressing which rules will remain, be altered or cease to exist after the EU legislation enters into force.

Protecting information on protective measures taken by communication providers of which the public availability could enhance the misuse of such services

The Authority can request information on preventive measures taken by hosting providers to adhere to their duty of care (Article 8(2)) and investigate communication providers unannounced for the presence of CSAM (Article(2)(b)). Such information obtained by the government may become public in response to Freedom of Information Requests (Wob-verzoeken). Although the explanatory memorandum clearly states that the Authority will focus its time and resource on communication providers who fail to take protective measures, we would like to point out that if information on protective measure taken by communication providers becomes public, this will help abusers to circumvent such measures and therefore possibly be detrimental to the combat of CSAM. In case of Freedom of Information Requests (Wob-verzoeken) related to this information obtained by the Authority, such requests should either be refused to protect the public interest or information on protective measures taken by communication providers against illegal content should not be provided.