



**YLVA JOHANSSON**  
MEMBER OF THE EUROPEAN COMMISSION  
HOME AFFAIRS

Rue de la Loi, 200 B-1049 Brussels  
Tel. [REDACTED]  
[cab-johansson-contact@ec.europa.eu](mailto:cab-johansson-contact@ec.europa.eu)

Brussels, 12/08/22  
*Ares sv(2022)6178475*

Dear [REDACTED],

Thank you for your letter of 05 May 2022 addressed to President Von der Leyen, Vice-Presidents Vestager, Jourová, Šuica and Schinas, as well as Commissioner Breton, on the EU proposal to prevent and combat child sexual abuse online. We welcome and share your engagement in the protection of fundamental rights and freedoms in our Union. The protection of the privacy, security and freedom of expression of all internet users is essential, and so is the protection of the fundamental rights of our children, including their rights to the integrity of the person and to privacy, which are severely violated by online child sexual abuse.

Taking action to combat child sexual abuse, including online abuse, as well as protecting children rights, is a priority for the Commission. This is highlighted in the EU strategy for a more effective fight against child sexual abuse adopted on 24 July 2020. This strategy contains eight core initiatives addressing funding, coordination and legislative needs across the Union. As a legislative initiative under this strategy, the Commission adopted on 11 May 2022 a new legislative proposal with the aim of providing an effective long-term solution to combat child sexual abuse online, including certain obligations for relevant online services providers to detect and report child sexual abuse online to public authorities.

We can – and must – pursue both protection of children against child sexual abuse and the protection of privacy of all users (including of the children subject to sexual abuse). The Commission's proposal strikes the right balance in this respect, notably by limiting any interference with privacy to what is necessary and proportionate, in compliance with the Charter of Fundamental Rights of the European Union and the case law of the European Court of Justice.

[REDACTED]  
[\[REDACTED\]@bitsoffreedom.nl](mailto:[REDACTED]@bitsoffreedom.nl)

In your letter, you refer to a lack of independent research on the effectiveness of technologies, that the proposal will undermine encryption, and that detection equates to nothing more than the automated scanning of everyone's communication.

Concerning your first point on detection technologies, the proposal ensures that these are only used to identify online child sexual abuse and that they are the least intrusive in accordance with the state of the art. The detection process is underpinned by a series of safeguards to address, amongst other things, the effectiveness of the technologies to be deployed. This includes the involvement of data protection authorities in the selection and application of detection technologies, the mandatory use of the database of online child sexual abuse indicators provided by the EU Centre, the attribution of the competence to issue detection orders to a judicial or independent administrative authority, and the provision of avenues for judicial redress for all actors whose rights might be affected during the process.

National authorities are explicitly required to take into account the availability of effective technologies capable of minimising any interference with privacy when deciding whether or not to issue a detection order. In addressing your second point on encryption, it is important to stress that the proposal should not be understood as incentivising or dis-incentivising the use of any given technology, since a balance between all fundamental rights at stake needs to be struck regardless of the technology used to provide interpersonal communication services. That includes the use of end-to-end encryption technology, which is an important tool to guarantee the security and confidentiality of the communications of users, including those of children.

Your third and final point concerning the prohibition of general monitoring speaks to the main focus of the proposal, which is to prevent online child sexual abuse, in particular through effective child safety by design features. Where a national competent authority, having assessed a particular service's prevention measures, considers that these measures are insufficient to the task, only then will that authority consider an application for a detection order.

Where a detection order is considered necessary, article 7 details the process to support the establishment of a balanced and targeted system, where the technologies to be deployed will be purpose limited, i.e. they will be limited to what is strictly necessary and proportionate to address the misuse of relevant information society services for online child sexual abuse. Furthermore, article 10 requires that providers deploy technologies that are the least privacy-intrusive in accordance with the state of the art in the industry, and that limit the error rate of false positives to the maximum extent possible.

In other words, detection under the proposal is a measure of last resort and subject to strict proportionality requirements. To ensure a correct balancing of all the rights and interests at stake in each case, the proposal entrusts the decision to order detection to a judge or other independent administrative authority.

In conclusion, the Commission's proposal aims to ensure full respect for the rights to privacy and data protection of children, and of others online. In the proposal, the detection of child sexual abuse is in line with data protection rules and privacy of communication rules, which require a proportionate legal basis. We thank you again for your input and look forward to further constructive engagement with stakeholders in our efforts to protect the fundamental rights of all our citizens.

Sincerely,



Ylva JOHANSSON