

To:

European Commission

Bits of Freedom
Prinseneiland 97hs
1013 LN Amsterdam
The Netherlands

Rejo Zenger
Policy advisor
+31 6 3964 2738
rejo@bitsoffreedom.nl

www.bitsoffreedom.nl
IBAN: NL73 TRIO 0391 1073 80
BIC: TRIONL2U
Chamber of Commerce: 34 12 12 86

Dear European Commission President Ursula von der Leyen,
Dear Executive Vice-President Margrethe Vestager,
Dear Vice-President Věra Jourová,
Dear Vice-President Dubravka Šuica,
Dear Commissioner Ylva Johansson,
Dear Commissioner Thierry Breton,
Dear Commissioner Margaritis Schinas,

Combating child sexual abuse is extremely important. In fact, it's so important that we cannot afford to put energy into measures to fight sexual exploitation of children that are controversial or ineffective. This problem, if possible even more so than others, requires a broad view and the application of proven and sustainable measures.

As we now understand, the Commission is planning to soon launch a proposal to tackle child sexual abuse online. We have reasons to believe that part of the proposal is an obligation that will force instant messaging service providers to monitor their users' communications. The intent would be to detect known and unknown material, as well as attempts at grooming. Providers are supposed to delete and report any suspicious material. Although the idea is noble, there are major drawbacks to the use of what is called *client side device scanning*:

- There is no independent research on the effectiveness of the technology used to detect child sexual exploitation material. The lack of independent research is disastrous because we cannot afford to invest in technology that has not been proven to be effective. At the moment, these kinds of technologies can mainly be described as experimental.
- Forcing providers to monitor what their users send and receive on their phones and computers undermines encryption. After all, the essence of end-to-end encryption is that a message can only be read by the sender and the intended recipient. This kind of technology is vitally important in today's society. In this particular context, end to

end-encryption is an important contribution to protecting the communication between, for example, a victim child exploitation and the counselor.

- In fact, such a measure is nothing more than the automated scanning of everyone's communication. This is by definition contradicting European law, such as the ePrivacy Directive and on a higher level, the Charter of Fundamental Rights. This means that, even if the proposal is passed, it will sooner or later be declared invalid by the European Court of Justice. The fight against sexual exploitation of children is far too important for a bet on controversial legislation.

This means that (parts of) the proposal is anything but sustainable and effective. As a result, the infringement of the right to privacy can never be proportionate. And that is even more relevant at a time when every aspect of our lives is becoming increasingly digital and the importance of a secure digital infrastructure is only increasing. The social costs of the measures in the proposal are therefore enormous. In our democratic society it is not appropriate to take measures *at all costs*.

We therefore call on you not to launch (these parts of) the proposal. Of course, that doesn't mean there is nothing the Commission can do. Tackling the sexual exploitation of children requires a broad set of measures. Focusing on technological solutions is not enough. For example, the Commission could focus on streamlining cross-border criminal investigations, increasing investigative capacity and taking more preventive measures that make young children more resilient. These types of solutions are not controversial and are at least as effective.

We are of course happy to contribute ideas about effective and sustainable legislation in this area.

Kind regards,

Rejo Zenger