

STOP CHAT CONTROL

The European Commission's Proposal published on 11 May 2022 includes severe threats to the right to privacy, including network blocks, upload filters, and mandatory chat control searching for all messenger providers; These measures would lead to the end of end-to-end encryption, the main guarantor of digital privacy, and they would overburden the police and public prosecutor's office throughout Europe.

LYMEC rejects the idea of the Proposal and the proposed measures as an infringement on the right to privacy, especially mandatory chat controls.

LYMEC instead calls for

- A holistic strategy to prevent and prosecute child abuse and depictions of child abuse which does not threaten the right to privacy and especially end-to-end encryption, for example the "notice and take down procedure" based on the US model.
- Better and closer cooperation of national security authorities within the EU, especially through Europol and Eurojust, and more investments for these agencies through the EU budget, but also with third countries, to successfully tackle the fight against depictions of child abuse across Europe.



LYMEC at the same time rejects other Proposals by the European Commission that disproportionately restrict civil rights in the alleged fight against crime, such as allowing identity determination through AI facial recognition in video surveillance.

The protection of privacy is recognised as a fundamental human right, and all users of modern technology should have control over their personal data.

LYMEC is in favour of the solutions that Big Data and IoT offer to some of the defining socio-economic challenges of the modern era, but recognises that they also bring an increased risk of abuse and fraud. Users seldom read privacy notices, do not always comprehend them fully, but consent to the processing of personal data nonetheless. Stronger, explicit consent mechanisms might actually have the effect that users will make less informed decisions about their privacy, or at least, it will not make their decisions more informed than they are now (consent transaction overload may lead to consent fatigue). Data privacy principles such as purpose binding and data minimisation may be difficult to reconcile with the constant development of big data technologies and software;

LYMEC urges

- ALDE to keep fighting for the fundamental right of privacy and data protection of its citizens both in its internal legislation and in its treaties and agreements with third parties.
- the EU should look towards practical and fair alternatives to the strengthening of consent-based autonomous authorisation model calls for further investment in research in the EU on technological developments in order to find solutions for these challenges proposed by the new digital environment in Europe and abroad.

