Terre des Hommes

CHILD PROTECTION & PRIVACY ONLINE

Scanning online messages and images for Child Sexual Abuse Material (CSAM) is considered by some as a privacy violation by default. But pitting child protection against privacy creates a false dilemma and oversimplifies the issue, as it does not reflect the reality of online safety, which requires detection of a wide range of risks. The necessary path ensures that **child protection and privacy to go hand-in-hand** to ensure online safety for all children.

PRIVACY & CHILD PROTECTION GO HAND IN HAND

Protecting children from online child sexual abuse and exploitation (OCSAE) is about ensuring strong safeguards and global standards for both privacy and protection of children online. The protection of children from OCSAE is enhanced by strong privacy protection, which is necessary to achieve children's online safety for several reasons.

SAFEGUARDING CHILDREN'S PRIVACY IS A KEY ELEMENT OF CHILD SAFETY BY DESIGN

Privacy plays a strong role in ensuring children's protection from OCSAE across all online services and platforms they use. Privacy settings can be used as **a safety tool to prevent OCSAE risks** from occurring**,** like grooming and sexual extortion. **Stronger privacy settings can guarantee higher online safety for children**, which can be done in ways that empower children:

Intelligent privacy by default settings include defaulting child users' profile to 'friends only' instead of 'public' to minimise interactions they may have with unknown people.

Proactive privacy features include features that encourage child users to proactively manage their privacy and to make safe choices.

Retroactive privacy features include giving children the agency to take action like untagging, blocking, reporting inappropriate content and behaviour after they occur.

Terre des Hommes

OCSAE IS A GRAVE VIOLATION OF VICTIMS' PRIVACY

The infringement of privacy seen as polarising to protection overlooks another crucial point: the fact that OCSAE and the dissemination of CSAM are **grave violations of the privacy of child victims and survivors.** As their abuse is recorded, their crime scene is memorialised. Each time their crime scene is shared or downloaded, not only is another crime being committed, a child is revictimised and retraumatised as they continually endure their abuse as it disperses online without their consent and control. As it circulates, their privacy continues to be violated. **Protecting children by detecting and removing their CSAM is therefore protecting their privacy.**

BALANCE PRIVACY AND PROTECTION TO DETECT CSAM

Detection technologies offer viable solutions when coupled with prevention efforts to protect child victims and secure their privacy. It is not contested that these technologies process users' data. Similar checks already exist on platforms when we agree to terms and conditions to scan our correspondence for viruses, phishing, terrorist content or inappropriate content. When creating legislation on detection, it is thus crucial to carefully assess legality, necessity, and proportionality to ensure no unlawful interference with privacy. This test is outlined using the Proposed EU Child Sexual Abuse (CSA) Regulation as an example on the next page.

The Right to Privacy (Art. 8 ECHR)

Article 8 of the European Convention on Human Rights (ECHR) safeguards the right to privacy, which is **not an absolute right.** This means it can be interfered with when:

1. It is **in accordance with the law**;
2. It is **necessary in a democratic society** in pursuit of a **legitimate interest.**

1) Is it in accordance with the law?

The Proposed EU CSA Regulation mandates the assurance of no automatic and unconditional monitoring of correspondence because of the limited circumstances and procedures when scanning is allowed. Through supervisory and judicial oversight and avenues for redress, it also assures this process is not independent of any judicial authority or due process (***Petra v Romania (ECHR)*** para. 37). The interference can thus be considered in accordance with law.

2) Is it necessary in a democratic society?

To assess this, the measure must pursue a legitimate aim and be necessary to achieve that aim in a democratic society (proportionality).

Terre des Hommes

Pursues a legitimate aim:

The case of ***Trabajo Rueda v. Spain*** (ECHR) held that police searching a personal computer prompted by a technician that found CSAM, pursued the legitimate aim of 'crime prevention' in protecting OCSAE victims.

Like this case, the aim of detection is to combat OCSAE by detecting, removing and investigating CSAM and grooming online. This goal aligns with the aims of **crime prevention** and for the **protection of the rights and freedoms** of others, particularly children to the right to protection from exploitation and abuse.

Proportionality: is the measure capable of meeting the legitimate aim?

Measures for detection, reporting and investigating would significantly reduce the violation of victims' rights by identifying them and stopping their ongoing abuse. This action reduces OCSAE, thus aligning directly with the aim of protecting children from exploitation and abuse.

Several policy options were examined throughout the Regulation's drafting process. The final impact assessment revealed that voluntary automated detection has insufficiently prevented OCSAE, with very few providers currently detecting CSAM. The chosen policy option, which mandates automated scanning and introduces safeguards to balance all rights, was thus justified as it best effectively meets the objective to combat OCSAE. This method, which cannot be achieved in a less privacy-intrusive way, is therefore proportionate for meeting the legitimate aims.

The European Court of Justice (ECJ) in ***Tele2 Sverige AB v. Post-och telestyrelsen*** and ***Secretary of the State for the Home Department v. Watson***, held that modern investigation techniques in the fight against serious crime, while crucial, cannot justify broad and indiscriminate retention of data.

Proportionality: balancing the interests at stake

The balancing of interests is reflected through various safeguards:

- There is **no general scanning.** Detection is limited to services misused for OCSAE after prevention efforts have failed to mitigate risks.
- The detection strategy and the tools used will need to be **approved** beforehand.
- Detection technologies are **built only for the purpose of determining whether an image is CSAM** or not through matching or classifying. As such, they are unable to read, understand or know the content of any image or video.
- Only **least privacy-intrusive** technology used.
- **Checks** by the independent EU centre to prevent false positives and reports.
- **Oversight mechanisms** to monitor power and independence of authorities issuing orders.

***Weber and Saravia v. Germany (ECHR)* held** that there was no breach of privacy with regards to strategic monitoring to identify and avert serious dangers as there were adequate and effective guarantees against abuses of the State's powers, and thus the privacy interference was proportionate.

- Affected service providers and users have the **right to effective redress.**

With these safeguards, the CSAM Regulation provides strict rules and oversight to ensure that adverse effects on the privacy of users are as limited as possible, while still achieving the objective of combating OCSAE.

For more information consult: Child Safety by Design 2022, CIP 2019, Eurobarometer Survey 2023, *Petra v Romania* App no 27273/95 (ECHR, 23 September 1998), *Trabajo Rueda v Spain* App no 32600/12 (ECHR, 30 May 2017), *Weber and Saravia v Germany* App no 54934/00 (ECHR, 29 June 2006), Joined Cases C-203/15 and C-168/15 Tele2 Sverige AB v Post-och telestyrelsen and Secretary of the State for the Home Department v Watson [2016] OJ C221, Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse COM/2022/20.