To ensure a safe internet for all – including children – the EU must pursue alternatives to the CSA Regulation

Despite the importance of its goals, the EU's proposed CSA Regulation 2022/0155 (CSAR) will not only fail in its aims to protect young people, it will even harm those it wants to protect. This explainer lays out key concerns and encourages policymakers to pursue ideas put forward by child rights groups for whole-of-society solutions to tackle the horrendous crime of child sexual abuse, rather than a harmful surveillance approach.

Based on our analysis, the legislative proposal fails to meet the key human rights principles of necessity and proportionality, violates several fundamental rights, and lacks a sufficient legal basis. As confirmed by the European Commission's own internal Regulatory Scrutiny Board (RSB), the CSAR may also violate the EU prohibition of general monitoring.

If passed in its current form, the CSAR would likely be struck down by the EU Court of Justice. We also raise many serious concerns about the technical and practical infeasibility of the highly-complicated proposal, along with procedural concerns that the proposed solutions could make it harder for law enforcement agencies to investigate and prosecute perpetrators of CSA. Lastly, we warn that the proposal fails to sufficiently engage with preventive and societal measures which could stop this problem from existing in the first place.

Along with 113 other civil society groups – including those working on children's digital rights, children's health, support for victims of online abuse, as well as the empowerment of girls and women – we call on the EU to withdraw the CSA Regulation and pursue alternative measures that are more likely to be effective, sustainable and fully respect EU fundamental rights.

The proposed CSA Regulation will have a disproportionate and severe negative impact on the following protections of *all* internet users – not just in the EU, but around the world:

1. **The right to privacy and the confidentiality of communications**
    - Under Articles 3-6 of the CSAR, virtually all digital communications providers (chat services, emails, telephone calls, app stores etc) will be required to take privacy-invasive measures to avoid Detection Orders. In many cases, this will require them to verify the ages of all users and may also require measures that would amount to the general monitoring of private communications. In some cases, providers will even be required to prevent under-18s from accessing legitimate messaging apps and services that they rely on to communicate with their friends and family;
    - Instead of starting with reasonable suspicion, as required by the rule of law, the measures in the CSAR will force private companies to treat every person as a potential suspect of CSA, thus also breaching the presumption of innocence. The extremely wide scope and reach of the proposal is at odds with the fact that most people who use digital communications services do so for legitimate reasons, including to exercise their political, cultural, economic and social rights;
    - Given the outcomes required by the CSAR, it will be impossible to target detection when scanning all forms of digital communication since, by definition, one needs to scan all messages of all users to find (potential) CSAM;
    - For those many young people whose abuser is a family member, preventing them from accessing private digital communications could prevent them from being able to escape their abuse, as noted by UN General Comment 25. Child protection experts point out that 90% of child abuse survivors are abused by someone known to them;

- The EU strategy (BiK+) accompanying the proposal suggests providing digital identity documents to under-18s (p.11) in order to support Articles 3-6 of the proposal. For undocumented young people, or those who face structural exclusion making it harder to access digital IDs, they could be locked out of digital communications;
- And as pointed out by the European Data Protection Board and Supervisor, measures in the proposed CSAR "may in fact harm even those they seek to protect."

2. Safe and secure communications

- End-to-end encryption is a vital tool for the protection of human rights. Under Articles 7-11 of the CSAR, Detection Orders can be issued which would require even end-to-end encrypted message providers to scan the content of people's private messages. The assessment of technical experts around the world is very clear: this simply cannot be done in a way that is safe, secure or respects the integrity of encryption,[1] and may even violate the *essence* of the right to privacy;
- Whilst the European Commission claims that Detection Orders are targeted, the draft CSAR allows for detection at a very large scale. For encrypted messages, it is impossible to target such measures, as by definition any interference with encryption will impact all users of that service – not just in the EU, but for anyone using that service globally;
- Experts warn that that CSS (client-side scanning) is not secure, does not comply with human rights, and creates back-doors into every person's digital devices – including those of children, making them more vulnerable to criminal networks;
- The US National Anti-Trafficking group Polaris warns policymakers not to see encryption as a "boogeyman" but as an important human rights tool, and instead to focus on the underlying social issues that lead to child abuse, exploitation and trafficking.

3. Freedom of expression – both online and off

- Articles 3-6 of the CSAR could lead to the widespread use of 'upload filters' which would scan every piece of content that people upload to their clouds, as well as public-facing digital conversations (like the chat functions in online games or social media posts). Such AI-based detection tools are notoriously faulty and inaccurate. Even when the accuracy is high, the volumes of material will lead to significantly more false reports than the EU Center and national law enforcement are able to process. Time will be spent analysing erroneous reports instead of investigating perpetrators;
- In the Impact Assessment that accompanies the proposed CSAR, accuracy statistics are provided at the word of private entities Microsoft and Thorn, and taken at face value with no independent validation;
- As we have already seen in China, there is no way to technically ring-fence these measures. Once they have been implemented in all digital services, and even on people's devices, repressive governments can require providers to scan for evidence of political dissidence, of people seeking reproductive healthcare and other legitimate actions;
- The measures in the CSAR will particularly impact journalists, whistleblowers, human rights defenders and anti-corruption advocates, as well as women and LGBTQI+ communities, which will have a chilling effect on free speech and democracy;
- In 2021, the UN General Assembly warned against the generalised surveillance of young people's digital communications. For teenagers, this would suppress their legitimate exploration online. As CSA survivor Alexander Hanff explains, surveilling survivors conversations can disempower them and ultimately discourage them from coming forward to report their abuse.

1 e.g. https://www.globalencryption.org/2022/05/joint-statement-on-the-dangers-of-the-eus-proposed-regulation-for-fighting-child-sexual-abuse-online/; https://www.politico.eu/article/europe-online-child-abuse-law-make-us-less-safe/; https://appleprivacyletter.com/; https://cepis.org/app/uploads/2022/03/Open-letter-on-a-right-for-encryption-CEPIS-2022-nosig.pdf; https://www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report

Instead of implementing surveillance measures that ultimately are likely to do more harm than good, we suggest that lawmakers focus on alternative, structural measures to tackling the root of the horrific crime of child sexual abuse, for example:

1. Education, awareness-raising and empowerment of survivors: Increasing awareness of and access by young people to hotlines, institutional reporting (police, social services and other authorities), and support mechanisms. Such interventions have long been encouraged in the work of chld protection organisations;[2]

2. Social and structural change: Many organisations recommend increasing investments in social services – especially child protection departments, schools, anti-poverty measures and other survivor / victim support services, as well as trauma-informed approaches by police;[3]

3. The reform of police and other institutions: In Germany, one of the largest vaults of abuse imagery ever discovered stayed online for years because police reported not having enough human resources to take it down. Yet it took journalists investigating the issue just a couple of days to fully remove the content.[4] Other Member States face similar issues, from the problem of closed institutions in France, to the overburdened police and public prosecutors in the Netherlands and Belgium. Structural solutions would ensure that the right authorities have the right resources to tackle the vast numbers of CSA cases that they are already unable to deal with;

4. Investment in hotlines: Increasing both EU and national funding to hotlines, ensuring a proper legal basis for their work, and committing funding further in advance, would boost the capacity and reduce the precariousness of these vital organisations who already remove vast amounts of CSAM from the internet quickly and effectively, and also provide support to survivors;

5. The enforcement of existing rules: The 2011 EU Child Sexual Abuse Directive contains many provisions requiring Member States to do more to tackle child sexual abuse on a national level, and worryingly, it has not been implemented fully despite being in force for over 11 years.[5] The DSA further offers many new opportunities to tackle illegal content online, including CSAM;

6. Prevention: "Abuse will continue if the root causes that allow it to exist in the first place are not challenged."[6] The CDC advises that "Effective evidence-based strategies are available to proactively protect children from child sexual abuse, but few have been widely disseminated";[7]

7. Working together to protect children *and* all fundamental rights: Bringing child rights groups, educators, social workers, digital rights groups, other human rights groups,will help us answer the real, pressing question: **how can we keep children safe while fully upholding fundamental rights?**

For more information, please see EDRi's 10 principles for protecting children in the digital age, as well as our document pool about the CSA Regulation. Our official analysis of the proposed CSA Regulation will be published in October 2022. For any questions in the meantime, please contact ella.jakubowska@edri.org.

2 https://ecpat.org/wp-content/uploads/2022/01/05-01-2022_Project-Report_EN_FINAL.pdf
3 https://www.ciase.fr/rapport-final/; https://www.who.int/publications/i/item/inspire-seven-strategies-for-ending-violence-against-children
4 https://netzpolitik.org/2022/depictions-of-child-abuse-the-internet-forgets-nothing-as-long-as-its-not-supposed-to-forget/
5 https://www.europarl.europa.eu/doceo/document/A-8-2017-0368_EN.html; https://ec.europa.eu/commission/presscorner/detail/en/inf_22_3768
6 https://home.crin.org/issues/sexual-violence
7 https://www.cdc.gov/violenceprevention/childsexualabuse/fastfact.html