EDRi 20

A safe internet for all

booklet

A safe internet for all: upholding private and secure communications

EDRi booklet on the human rights reasons to reject the proposed EU Child Sexual Abuse Regulation (CSAR) and demand better instead.

April 2023

It is not just adults that have a right to the privacy of digital communications, but children too, a concern which has been largely neglected in the Commission's proposal.

In March 2022, the European Commission put forward a proposal for a law which would create legal responsibilities for online service providers to tackle the spread of child sexual abuse material (CSAM) and online child grooming.[1]

If passed, this law would apply to virtually every digital communications service, from chat apps to social media, through o cloud services, app stores, and even text messages, phone calls and internet infrastructure services. Some EU governments also want to explicitly add search engines. Since 2002, EU law has been clear that these online communications and service providers cannot be forced to know the contents of their users' messages, calls, photo uploads and other personal content.

This is a basic tenet of democratic society, as the privacy that we are all entitled to offline applies equally so online. Just as the police cannot raid your house without a warrant, neither can police – let alone companies – go through the digital version of your private inner life without a specific, individual reason to believe that you have done something to justify this.

**Privacy is not an abstract concept or a barrier, but a vital human right.
Around the world, privacy rights and privacy-protective tools prove vital in ensuring that journalists can safely report on corruption, that human rights activists can hold power to account, that civilians can flee oppressive regimes, that LGBTQI+ people can stay safe, that people can freely practice their religion and access healthcare, and that democracy can thrive.**

[1] Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse' (2022/0155 COD), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN

To echo the European Data Protection Board and Supervisor, the proposed CSAR is likely to do great harm to regular people, with a very limited impact on stopping perpetrators of this terrible crime.[2] EDRi, along with 133 other civil society groups and counting, have called on the European Commission to withdraw the proposal.[3] We further call on the European Parliament and EU Member States to reject the proposal. This is based on our in-depth analysis, which has shown that: [4]

- **Detection Orders cannot be sufficiently targeted, and instead will usually mandate the generalised scanning of private digital communications**, which amounts to mass surveillance and can dangerously undermine encryption. No amount of innovation or technological development can change this, as it is a fundamental feature of how detection technologies work;
- It is likely that if passed, the intrusive scanning obligations entailed by Detection Orders would be considered **unlawful general monitoring** by the Court of Justice of the EU;
- Risk assessment and mitigation measures will heavily incentivise the use of so-called 'upload filters', which can **enable digital censorship and suppress free expression;**
- These risk measures will also require the widespread use of age verification methods which could **put the personal data of children and adults at risk,** exacerbate social exclusion and eliminate the possibility of online anonymity;
- As a result, the CSAR is likely to both **undermine, and create regulatory overlap, with the Digital Services Act (DSA).** It is also likely to **disproportionately infringe on the privacy, data protection and free expression rights of potentially the entire European** population, in contradiction to the Charter of Fundamental Rights;
- The proposed model will be cumbersome, **lacks evidence of effectiveness, and may even be counterproductive** at achieving its stated goals of protecting children;

[2] EDPB and EDPS Joint Opinion on the CSAR: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-042022-proposal_hu

[3] The call from civil society groups to withdraw the CSAR: https://edri.org/our-work/european-commission-must-uphold-privacy-security-and-free-expression-by-withdrawing-new-law/

[4] EDRi's full position paper: https://edri.org/wp-content/uploads/2022/10/EDRi-Position-Paper-CSAR.pdf

- The technological methods required to implement the CSAR will lead to **high levels of false alarms, making it harder to investigate actual cases** of CSA, whilst putting the devices of adolescents and other innocent internet users at an increased risk;

- A sustainable alternative to the CSAR is to f**ocus on the fast removal of CSAM from the internet.** This would be better achieved by a combination of:
    - Strong and effective DSA notice-and-action implementation;
    - The creation of obligations on platforms and services to ensure users can always report CSAM in ways that are both child-friendly and effective; and
    - By giving a legal basis to and increasing investment in national child protection hotlines, as well as to dramatically increase awareness of their existence and how to access them;

- Such measures must be underpinned by meaningful societal change, reforms of **criminal justice institutions, education** and a far greater **investment in primary prevention of CSA.**

Contents

1. What would change compared to today as a result of the CSAR?

There is a temporary EU law in force which allows digital communications services to scan the private communications of their users based on their terms of service.[5] This law has been criticised by civil society and legislators for likely being in conflict with the General Data Protection Regulation (GDPR) and for encouraging general monitoring of people's communications. It has also been criticised for failing to meet key human rights standards, for being completely opaque, and for giving too much discretion to private entities.

The European Commission has agreed that it is necessary to replace this problematic temporary law with a long-term law. However, despite public assertions from the Commission that if the new law is not adopted by 2024, children will be left with no protections, this is simply not true.

Most importantly, the Digital Services Act (DSA) has now entered into force, and will become fully operational by early 2024. This new law creates a wide range of methods to deal with illegal online content, including CSAM. The Commission has also confirmed in writing that if they had to, they could extend the temporary law. A manufactured sense of urgency, therefore, does not help anyone:

children are relying on EU legislators to take sufficient time and care to find ways to protect them that are safe, effective, and lawful. The proposed CSAR is unlikely to meet any of these three criteria.

One of the main changes from the temporary law to the CSAR is that the proposed new scheme is mandatory. Risk assessment and mitigation measures will be largely universal, whilst scanning requirements will apply only after the issuance of a Detection Order.

[5] https://edri.org/our-work/a-beginners-guide-to-eu-rules-on-scanning-private-communications-part-1/

That means that whilst providers could previously choose whether or not to scan content, they could now be forced to do so, even if that would require them to downgrade the security of their service to make this possible, or to break the trust of their users. As a result, **the biggest change from today would be that potentially any service or platform operating in the EU could be forced to monitor and scan the content of their users' entire digital lives.**

2. What are the main new rules in the CSAR?

Several of the proposed new rules in the CSAR have deep implications on the human rights and digital safety of all internet users – including young people, who increasingly rely on the internet to communicate with friends, build communities, connect for activism as well as for education and access to services.

2.1 Risk Assessment and Mitigation (Articles 3 and 4)

Articles 3 and 4 of the CSAR require virtually every digital or online platform or service to identify and reduce the risk of CSAM being exchanged, or children being groomed, on their platform or service. This means that providers will need to know what is being said or shared on their platform or service at all times, even if that means systematically monitoring their users' content. What's more, the platforms or services will still be considered "significantly" risky unless they can show that the exchange of CSAM and incidences of grooming are eliminated "beyond isolated and relatively rare incidences" (Recital 21).

These measures will require private entities to take a state-like role in deciding what content is acceptable and what is not. This will also strongly incentivise providers to take the most intrusive measures possible in order to avoid a Detection Order.

The scanning of public-facing communications (sometimes referred to as 'upload filters') and the over-removal of legitimate content will therefore become the norm. These filters are notoriously faulty, which is a problem because of how serious a false allegation of CSA can be. Upload filters have also been linked to a severe interference with freedoms of expression and access to knowledge, and a high risk of re-purposing for censorship and repression.

What's more, access to virtually all online platforms and services could become contingent on proving your age. This can have major impacts on freedom of expression and data protection rights, as well as preventing access to social, economic and political rights. The three main methods of age verification that currently exist are:

- **Requiring users to upload an identity document, such as a passport scan**. Such a scheme would make online anonymity impossible, which can put everyone from journalists to whistle-blowers to sex workers at risk, and excluding those without formal ID;
- **Implementing a wide-scale digital identity system**. Digital identity systems risk further marginalising people who already face high levels of social exclusion, such as undocumented people, homeless people, Roma communities and elderly people. The EU is currently pursuing a digital identity scheme (eID), and civil society have raised serious concerns about plans to use this system also for surveillance advertising, the fact that there are currently no guarantees that this system will respect privacy, and the fact that at least 20% of the EU population is predicted to be excluded from the scheme;
- **Using facial recognition or other algorithmic profiling to predict ages of users.** These systems are notoriously inaccurate, especially for people of colour and people with facial differences. By definition, such methods will also routinely process the incredibly sensitive biometric data of young people. Many of these systems are being used already in commercial contexts, profiting from the data that they gather.

Despite these risks and abuses, it is becoming more and more common for policymakers to encourage the widespread use of age verification tools, without considering the systemic violation of children's rights that their use entails.

2.2 Detection Orders (Articles 7 - 11)

Articles 7-11 of the CSAR lay out the rules for how national coordinators can request judicial or administrative authorisation to force providers to scan ("detect") their users' messages or other content. There are three types of content that they could be requested to scan for:

- **Known CSAM**, usually images or videos that have been previously reported, reviewed and then put into a database. This is sometimes referred to as a 'hash database' or 'hash matching' because scanned content is compared to a reference ('hash') of known CSAM. Whilst the creators of these databases and scanning technologies claim that they are highly accurate, there has been no independent verification of this, and research shows that the hashes can be inverted to reveal the original abuse imagery;[6]
- **New CSAM**, meaning images that have not been previously reported as CSAM or put in a hash database. This requires the use of artificial intelligence (AI)-based technologies, which can be trained to look for 'indicators' (e.g. predicting if an image shows bare skin). This means that such tools will never flag only CSAM, but will flag any material that fits the search criteria;
- **Solicitation (or grooming),** meaning text, audio or behaviours that could indicate that someone is grooming a child. Again, this requires the use of AI-based technologies to look for patterns or other alleged 'indicators' of grooming.

[6] https://gangw.cs.illinois.edu/PHashing.pdf

Detection Orders are the online equivalent of putting a recording device in homes across the EU, and then using AI-based tools to predict if audio or video content might indicate child sexual abuse.

Despite the CSAR's attempts to use Detection Orders only in specific circumstances, there is no way to target them only against suspects. That is because when it comes to private communications, you cannot know who is a suspect until everyone's content has first been scanned.

The proposed CSA Regulation requires these Orders to be targeted in terms of content and technologies, but not in safeguards or scope. This means that Detection Orders will almost always have to routinely scan the legitimate content of lawful internet users, rather than being specifically targeted against only those users where there is a reasonable suspicion of illegal conduct.

As a result, it is likely that the proposal will constitute a general monitoring obligation, which the Court of Justice of the EU has repeatedly held is illegal.[7]

Whilst such a mass surveillance approach would inevitably lead to some cases of CSA being flagged, the unacceptable invasion of people's private lives is made very clear by the home recording device analogy.

What's more, the vast majority of what these scanning systems would catch would be false alarms, especially for unknown CSAM and grooming. This is because at the volumes of material being scanned, even highly accurate technologies will catch in their wide net a lot of legitimate content.

This will make finding actual cases of CSA like finding a needle in a haystack, making it likely that authorities – who are already over-burdened and under-resourced – will have less capacity to protect victims and punish perpetrators.

[7] The prohibition of general monitoring obligations is clearly asserted in the ePrivacy Directive (2002) and the Digital Services Act (2022). It has also been reinforced in judgements from the Court of Justice of the EU, for example La Quadrature du Net and others (joined cases C-511/18, C-512/18 and C-520/18), Schrems I (C-362/14), Digital Rights Ireland (joined cases C-293/12 and C-594/12) and Poland v Parliament and Council (C-401/19).

There is also a problem here with what is meant by 'accuracy'. Scanning technologies can be tuned to be highly accurate at detecting skin, for example. That doesn't mean that they are highly accurate at detecting CSAM: images containing skin might be a picture of a 20-year old in a swimsuit, or a close up of a teenager's arm. The CSAR proposal claims that a prominent scanning technology, 'PhotoDNA', is highly accurate. However, when used by networking platform LinkedIn, only 41% of the images that were flagged by PhotoDNA in 2021 actually constituted CSAM under EU law.[8]

When it comes to detecting new CSAM and grooming (solicitation), this relies on the use of artificial intelligence (AI) technologies such as machine learning. It's not a question of the technology needing to get better over time. It's the fact that what constitutes CSAM or solicitation can be highly dependent on context.

For example, several EU countries decriminalise the sharing of sexual imagery between consenting teenagers, but an AI-based tool cannot know the difference between these different national legal frameworks.

Context is vital in distinguishing between unlawful CSA and legitimate expression, and machine-learning technology cannot understand context, as it has no common sense.

2.3 Blocking Orders (Articles 16-18)

Articles 16–18 of the CSAR allow authorities to force internet access providers to block access to a URL (web page), for example because a non-EU site is hosting CSAM, meaning that the EU does not have the power to demand the content's removal. A major issue with Blocking Orders is that it is simply not possible for most internet access providers to block a particular URL. They do not have access at the level of the URL, only the entire website (domain). This means that, for example, if just one page on a large site like Reddit was found to contain CSAM, the EU could force internet access providers to block access to every single Reddit page, for every person in the EU. This would have a severe and disproportionate impact on freedom of expression and the right to access information.

[8] https://edri.org/our-work/internal-documents-revealed-the-worst-for-private-communications-in-the-eu-how-will-the-commissioners-respond/

How do detection orders work?

CSA
REGULATION

Article 7.

Issuance of Detection Orders

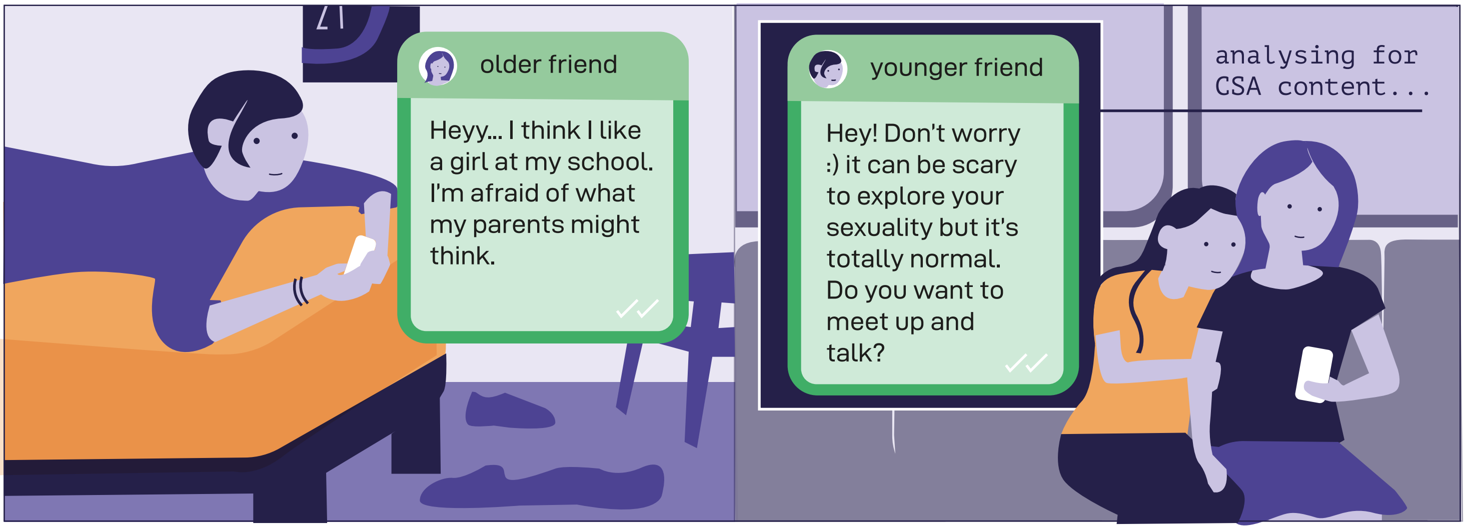
- "[where] it is likely … that the service is used, to an appreciable extent for the dissemination of … child sexual abuse material"
- "[when] the reasons for issuing the detection order outweigh negative consequences for the rights and legitimate interests of all parties affected"

A national administrative authority issues a detection order to a company

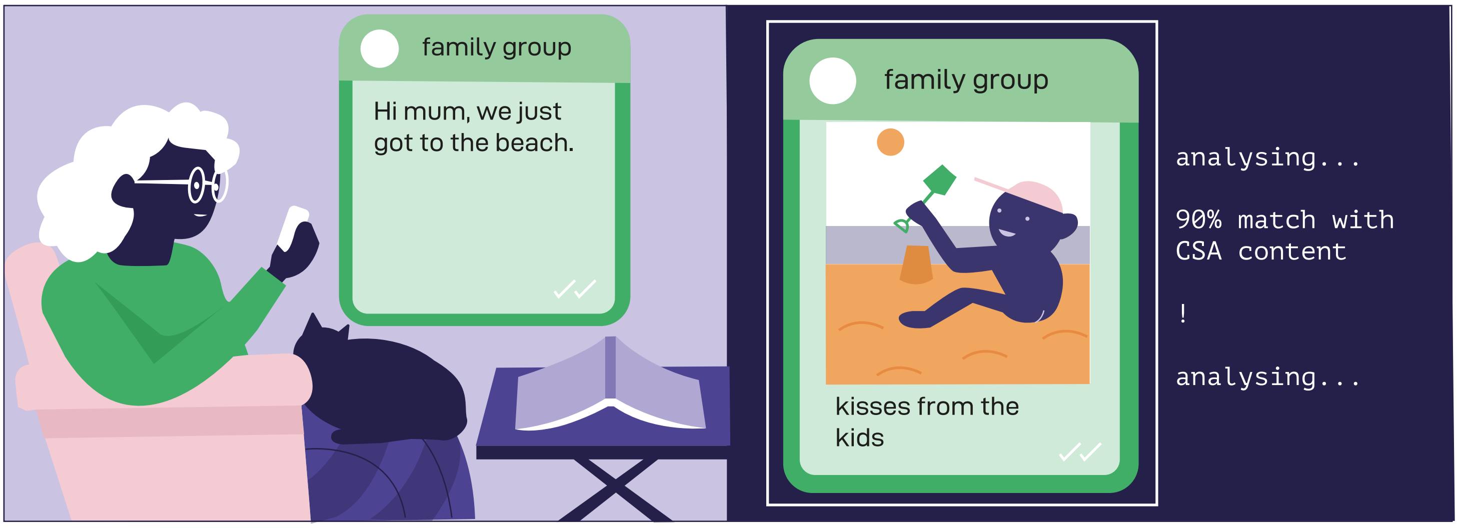
The company is obliged to use AI tools to look for child abuse material or grooming in the chats of its users. This even applies to encrypted messages.

This undermines the encryption and makes the messages of all users less secure.

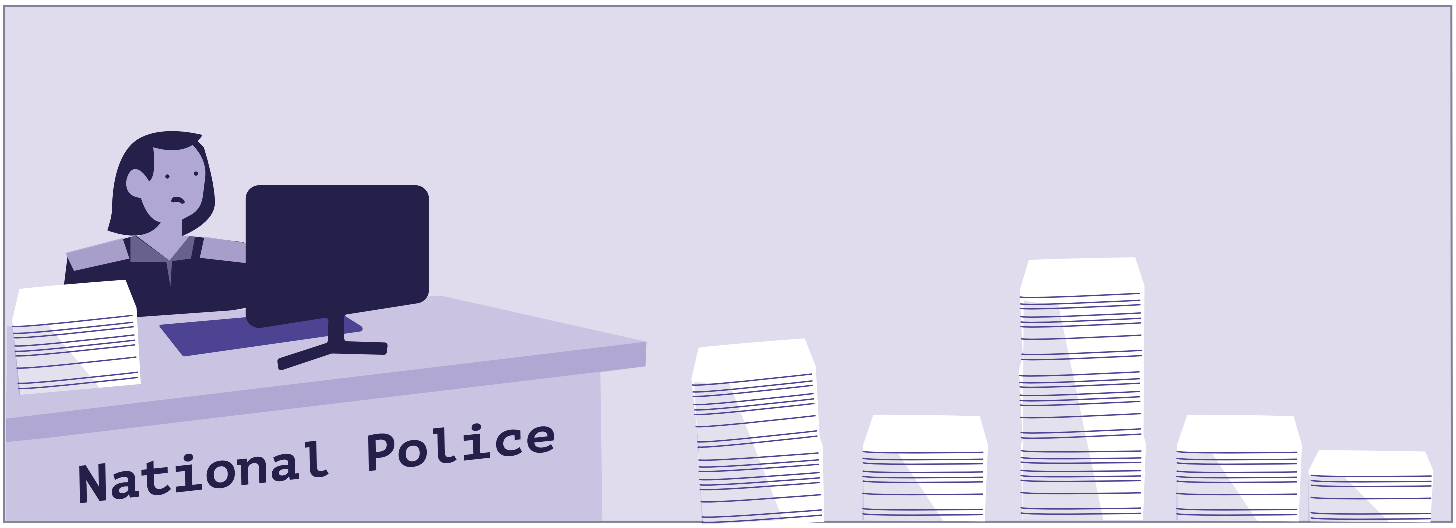
Becoming an additional risk for LGBTQI+ people.


older friend
Heyy... I think I like a girl at my school. I'm afraid of what my parents might think.
younger friend
Hey! Don't worry :) it can be scary to explore your sexuality but it's totally normal. Do you want to meet up and talk?
analysing for CSA content...

Falsely accusing innocent people of crimes



taking valuable time from police to look for real perpetrators.



3. How would encryption be affected?

The CSAR is not a technologically-neutral proposal. Whilst it does not mandate specific technologies that providers will have to use in order to comply with the law (this will be left to a list managed by EU Center), there are certain technologies that inevitably will be used or impacted.

The most prominent technology that will be impacted is encryption. By not having an exception from Detection Orders for end-to-end encrypted (E2EE) services, providers of secure message services could be forced to scan the content of their users, contrary to their commitment to respect their users' privacy. This is technically very different from existing scanning practices for 'malware', for example, which do not impact the content or integrity of those E2EE services. It is therefore not accurate to compare these practices to the scanning that would be required by a Detection Order.

Worryingly, the CSAR explains that encrypting communications is one of the factors most likely to make a service be considered risky (and therefore likely to receive a Detection Order). It is foreseeable that under the CSAR, most E2EE services (which the United Nations High Commissioner for Human Rights reminds us are an important human rights tool)[9] would either have to leave the EU, or face a Detection Order.

Complying with a Detection Order is technically not possible without undermining the security and fundamental premise of an E2EE service, meaning that the CSAR would clearly undermine encryption. All currently-known methods to do this would require either weakening the encryption directly, or introducing 'Client-Side Scanning' (CSS), which has been roundly criticised by the cybersecurity and human rights community for making people's devices vulnerable to malicious actors, as well as to manipulation.[10]

The European Commission's Impact Assessment to the CSAR recognises that even state-of-the-art methods have at best low-medium levels of privacy and security, and have never been successfully deployed at scale.

[9] https://www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report
[10] https://arxiv.org/abs/2110.07450; https://privacyinternational.org/sites/default/files/2022-09/SECURING%20PRIVACY%20-%20PI%20on%20End-to-End%20Encryption.pdf

Even if a safer and more secure technique than CSS were discovered in the future, this would not overcome the fact that any detection method rolled out in E2EE environments is fundamentally incompatible with the point and purpose of E2EE. This is because it would bring a third party into a communication that is supposed to be only between the sender and the recipient.

That commitment to privacy is what ensures that human rights defenders, politicians, lawyers, people seeking reproductive healthcare, activists, people living under authoritarian regimes and many others can rely on E2EE services to stay safe.

What's more, that third party would be obligated to refer any content that the detection tools predict as CSAM or grooming to police, including inevitably high volumes of lawful and legitimate content.

Crucially, there is no way to turn the E2EE on and off for certain users. As a result of a Detection Order given to an end-to-end encrypted service, every person relying on that service would have their privacy and security compromised.

This cannot be avoided as it is a technical feature to ensure the safety of E2EE. This would therefore also have an impact on that platform or service's users outside the EU.

Every device subject to CSS will be made technically much more vulnerable to attacks and hacking by a wide range of malicious actors.

4. The problem of effectiveness and efficiency

Beyond the technological limitations of the methods that would be required to meet obligations under the CSAR, there are several procedural reasons why it is unlikely to be effective:

- The vast majority of enforcement of the proposal will fall to Ireland and the Netherlands, as most of the EU's digital services are registered in those two territories. With backlogs in GDPR enforcement already reaching several years, creating the same process for CSA will create severe delays that we cannot consider acceptable when children's safety is at risk;
- Decentralised models of content removal – such as by national hotlines or by trusted flaggers under the DSA's future notice-and-action mechanism – are considered best practice in swiftly taking down CSAM. Fast removal is widely accepted as best practice for preventing CSA survivors from being re-victimised by the onward sharing of imagery. By contrast, a study on centralised models (which is what the EU Center would be) shows that they can add up to 6 weeks to the time it takes to remove CSAM from the internet.[11] This means that the CSAR is unlikely to be the most effective way of achieving its main aim of stopping the further dissemination of CSAM online;
- The CSAR requires every piece of suspected CSAM that is not "manifestly unfounded" (for example, a picture of a kitten that has been mistakenly flagged as CSAM) to be reported to national police for investigation. Given the high likelihood that much of the reported content will actually be legal and legitimate content, it will be a huge waste of (already limited) police resources to have to investigate each time a teenager consensually sends a topless selfie or a parent sends a beach picture to their child's grandparents; [12]

[11] https://www.lightbluetouchpaper.org/2022/05/11/european-commission-prefers-breaking-privacy-to-protecting-kids/

[12] As explained by child rights expert Dr Sabine K Witting, this could in fact put young people at serious risk of harm and violation of many of their rights: https://netzpolitik.org/2023/csam-verordnung-chatkontrolle-verletzt-sexuelle-selbstbestimmung-von-jugendlichen/ [in DE]

- The Netherlands' police commissioner has confirmed that Dutch police would be unable to deal with the volume of grooming reports that they would expect to receive as a result of the CSAR; and a senior German police officer in charge of investigating CSA similarly said that "chat control" will not help find more perpetrators, only more false alarms. This demonstrates that even law enforcement on the front lines do not see the CSAR as likely to help in their fight against CSA..[13]

5. How will legitimate internet users be affected?

Most people use the internet for legitimate, lawful and important reasons: work, communicating with family, storing cherished photos, chatting with their partner, building communities, justice, seeking information, keeping in touch with friends, providing or accessing healthcare, mobilising for social change, expressing themselves and

more.

The fact that a minority of users abuse digital channels for heinous purposes does not mean that every person should be routinely treated as suspicious, as EU law asserts that we are all entitled to the presumption of innocence.

Child protection groups explain that online strangers are not the main demographic of CSA perpetrators: **"While commonly held perceptions tend to frame sexual abuse both online and offline in terms of 'stranger danger', in reality children face more frequent risk of harm from people within their circles of trust."**[14] The CSAR's proposed general online surveillance model therefore is not only misaligned to the main ways in which CSA is committed in reality, but will also have disproportionate impacts on the general public:

- We are already seeing innocent people being locked out of their digital lives as a result of scanning technologies falsely claiming that they've spread CSAM. More and more reports are coming out of people losing every single photo they've ever uploaded to the cloud, being permanently locked out of their email accounts and password managers, with huge impacts on their ability to work, communicate and engage in digital life.

[13] https://debatgemist.tweedekamer.nl/node/29579; https://www.deutschlandfunk.de/strafverfolgung-sexueller-kindesmissbrauch-datenschutz-100.html

[14] https://ecpat.org/wp-content/uploads/2022/01/05-01-2022_Project-Report_EN_FINAL.pdf

Anecdotal reports suggest even graver consequences for other people on the basis of false accusations, including the loss of jobs, loss of families and suicide by those that are falsely accused;

- Our full report reveals that in Ireland, hundreds of people have had their data retained by police (which is likely illegal) despite being cleared of any CSA crime. In fact, what these people had shared was legitimate content: this included family photographs of their children playing on the beach and consensual sexual images between adults;

- The severe impacts of general surveillance are often referred to as the 'chilling effect'. Just knowing that your conversations, emails and uploads might be systematically monitored can suppress people's rights to express themselves, to seek information, and to assemble and associate freely (for example, to engage in political activities or activism);

- In countries which lack a strong rule of law, the risks of misuse and so-called 'scope creep' can also be high. For example, 'upload filters' can be repurposed to seek out legitimate content (such as evidence of political dissidence, critical journalism, or people searching for reproductive healthcare);

- The internet is global. By undermining digital privacy, security and safety in the EU, the CSAR could encourage providers to also weaken the security and increase the surveillance for their users around the world. There is also the fact that by giving a carte blanche to such surveillance methods, the EU is giving a signal to countries around the world that these measures are acceptable.

6. What does child rights law say?

International and European law puts obligations on states to protect children from sexual abuse, a horrific crime which violates several of children's fundamental rights.

The Council of Europe Lanzarote Convention also requires that children's best interests must be a primary consideration. This does not mean, however, that any measure to protect children will automatically be acceptable.

Many of the arguments in favour of the CSAR have highlighted the severity of the crime of CSA. This proves that governments must act to protect children, but not that the CSAR is necessarily the right way to act. Child protection measures, as important as they are, still need to be necessary, proportionate and lawful measures in a democratic society.[15]

Child rights law also requires governments to consider children's views and wishes as well as potential consequences on their rights and freedoms. The UN, UNICEF and Child Rights International Network (CRIN) all emphasise that generalised online surveillance of children can be harmful to their development and self-expression.[16]

Our analysis has shown that this risk could be especially profound for LGBTQI+ young people, who will find that the legitimate exploration of their sexual self-identity is treated as if it is criminal behaviour, and that such intimate content is routinely shared with platforms and law enforcement.[17]

CRIN adds that the most effective online safety mechanism is to ensure empowered, resilient young people who feel confident to speak up when something makes them concerned..[18] Several survivors of CSA also point to the importance of online privacy for seeking help and building a sense of community and hope.[17] This could be eradicated by the CSAR, which runs the risk of flagging survivors confiding in others as CSAM, and removing any sense of safe spaces thanks to the constant threat of surveillance. That's why several groups representing survivors of various forms of online abuse as well as children and young people's rights have joined EDRi's call to withdraw the CSAR.[19]

[15] This is especially the case given that the CSAR places obligations onto private companies and individuals. This means that the obligations are 'positive' obligations to protect children from harm, which are not absolute (meaning the state cannot do anything at any cost to achieve this obligation), compared to 'negative obligations' which are absolute (e.g. the state can never abuse children).

[16] See especially UN General Comment 25: https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC%2FC%2FGC%2F25&Lang=en

[17] Child rights expert Dr Sabine K Witting advises that the search for unknown material is removed from the scope of the CSA Regulation in order to remove this serious risk: https://netzpolitik.org/2023/csam-verordnung-chatkontrolle-verletzt-sexuelle-selbstbestimmung-von-jugendlichen/ [in DE]
https://home.crin.org/issues/digital-rights/childrens-right-digital-age?rq=digital%20age

[18] https://www.linkedin.com/pulse/why-i-dont-support-privacy-invasive-measures-tackle-child-hanff

[19] See EDRi's open letter calling to withdraw the CSAR as well as the Stop Scanning Me campaign: https://edri.org/our-work/european-commission-must-uphold-privacy-security-and-free-expression-by-withdrawing-new-law/ and https://stopscanningme.eu/en/

7. What does EDRi recommend instead?

We call for the EU's resources to be directed at the minority of people who use any methods – digital or otherwise – to commit, facilitate or spread CSA. **This can include genuinely targeted, lawful measures to investigate the minority of users who misuse encrypted services for committing CSA and other serious crimes.**[20] The US anti-trafficking hotline warns that encryption should not be seen as a "boogeyman" and that the focus instead needs to be on the underlying practices whereby traffickers and abusers exploit vulnerable individuals or communities.[21]

Genuine, sustainable change requires political commitment to and investment in driving a societal transformation which treats survivors with dignity, which facilitates swift access to justice, which refuses to look away when abuse is suspected, which offers mental health support to those dealing with CSA cases and CSAM in any capacity, and which prioritises research into prevention to stop the awful crime of CSA in the first place. Far less invasive, and likely more effective and efficient methods for tackling CSA both offline and online, include the following (and could also be implemented much sooner than the CSAR, therefore also being in the best interests of survivors):

- Prioritising the implementation of the Digital Service Act (DSA) removal (notice and action) mechanisms for illegal content, including properly equipping trusted flaggers;

- Ensuring all platforms and services in the EU have a clear, accessible, child-friendly way for suspected CSAM to be reported, and that response teams are adequately resourced to be able to respond in a fast and effective manner;

[20] EDRi position paper, 'State access to encrypted data' (2022): https://edri.org/our-work/breaking-encryption-will-doom-our-freedoms-and-rights/

[21] Quote from Polaris (US national anti-trafficking hotline): "The debate is not around whether or not encryption is good or bad. It's about how are traffickers exploiting vulnerabilities of vulnerable communities, and where are they doing that, and how do we actually get ahead of that vulnerability and meet that need. I think there's oftentimes a bit of a boogeyman made around emerging technologies. Technology is just a tool in which [crime] happens, but the underlying mechanisms need to be understood at its very core." Rajan said that she believes encryption is part of a "human rights toolkit" that can protect and empower victims. She posed the question: "How do we prevent abuse of these technologies rather than passing a broad, sweeping critique of a tool?" Available at:https://www.cnbc.com/2022/06/10/wickr-amazons-encrypted-chat-app-has-a-child-sex-abuse-problem.html

- Investing in and giving a clear legal basis to proven services like national hotlines, as well as making sure that children and young people are familiar with what the hotlines are, how they can help them, and how to get in touch;

- Ensuring all platforms and services in the EU have a clear, accessible, child-friendly way for suspected CSAM to be reported, and that response teams are adequately resourced to be able to respond in a fast and effective manner;

- Investing in and giving a clear legal basis to proven services like national hotlines, as well as making sure that children and young people are familiar with what the hotlines are, how they can help them, and how to get in touch;

- Pursuing ambitious social reforms, including around welfare, anti-poverty measures, social services, police reform and judicial reform;

- Focusing on the education and empowerment of young people to use the internet safely;

- Pursuing the full extent of existing law, including the 2011 Child Sexual Abuse Directive (which has not been fully implemented in many Member States);

- Addressing the societal factors that enable CSA, including harmful gender norms about women and girls, and broader issues of social inequality;

- Ensuring the consistency of criminal record checks, training and awareness of the signs of CSA for everyone working with children and young people;

- Increasing research funding and capacity into prevention, as well as swiftly implementing prevention methods, in order to prevent CSA crime before children are harmed. The potential for harm reduction by focusing on prevention is enormous but usually overlooked.

Under human rights law, it can be necessary and acceptable to limit the privacy and data protection of those who are suspected of serious crimes such as child sexual abuse. There are even technological methods to support investigations in such cases which – as long as they follow due process rules and respect human rights principles – can be compatible with the rule of law.

We urge legislators, therefore, to distinguish between interventions and measures which are targeted against suspects, and are therefore legitimate, compared to those that have a profound impact – whether deliberate or unintended - on an entire population (e.g. upload filters, many forms of age verification, and detection of content in private messages) and should therefore be rejected.

The full legal and technical analysis that underpins this booklet is available at:
https://edri.org/wp-content/uploads/2022/10/EDRi-Position-Paper-CSAR.pdf

We also recommend additional resources on how states can pursue lawful investigations against those suspected of serious crime such as CSA:

- 10 Principles to Defend Children in the Digital Age (2022): https://edri.org/our-work/chat-control-10-principles-to-defend-children-in-the-digital-age/

- State Access to Encrypted Data (2022): https://edri.org/our-work/breaking-encryption-will-doom-our-freedoms-and-rights

Mass surveillance. Random Censorship. Content Restrictions.

Companies and governments increasingly restrict our freedoms.

—

DONATE NOW:

https://edri.org/take-action/donate

Press enquiries
press@edri.org

Brussels office
brussels@edri.org

Phone number
+32 2 274 25 70

Visit us
Rue Belliard 12
1040 Brussels
Belgium

Follow us
Twitter
Facebook
LinkedIn
Youtube

EDRi

European Digital Rights (EDRi) is the biggest European network defending rights and freedoms online. We promote, protect and uphold human rights and the rule of law in the digital environment, including the right to privacy, data protection, freedom of expression and information.

www.edri.org

Designed by Gemma Portella - www.gemmaportella.com - gemma@gemmaportella.com