Deutscher Bundestag
Ausschuss für Digitales

Ausschussdrucksache
20(23)137

28.02.2023

Written responses to questions from Bundestag in advance of 1 March hearing

Ella Jakubowska, Senior Policy Advisor, European Digital Rights (EDRi)

27 February 2023

The EDRi network is a dynamic and resilient collective of NGOs, experts, advocates and academics working to defend and advance digital rights across the continent. For almost two decades, it has served as the backbone of the digital rights movement in Europe.

1. The European Commission's proposal for a CSA Regulation, also known as the "chat control" proposal, has been the subject of a great deal of discussion since its publication in May 2022. Please explain the technical, legal, fundamental-rights, data-protection, social and/or societal implications of the proposal.

EDRi's assessment is that the European Commission has put forward a proposal which, if passed, would likely violate several rights in the EU Charter of Fundamental Rights; the recently-adopted Digital Services Act (DSA); the General Data Protection Regulation (GDPR); and the prohibition of general monitoring obligations, which has been maintained repeatedly by the Court of Justice of the European Union (CJEU). We note that the Commission's own internal 'Regulatory Scrutiny Board' expressed several reservations about the proposal, including their concern that the proposal does not sufficiently explain how it can comply with the prohibition of general monitoring.[1] The United Nations Commissioner for Human Rights has also raised the same concern about general monitoring.[2]

1 The opinion of the Commission's Regulatory Scrutiny Board (RSB) was leaked in 2022, showing several concerns about the proposal from within the Commission,. EDRi, 'Leaked opinion of the Commission sets off alarm bells for mass surveillance of private communications, 23 March 2022, available at: https://edri.org/our-work/leaked-opinion-of-the-commission-sets-off-alarm-bells-for-mass-surveillance-of-private-communications/.

2 UN Office for the High Commissioner for Human Rights, 'Spyware and surveillance: Threats to privacy and human rights growing, UN report warns', 16 September 2022, available at: https://www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report.

This draft law would constitute a level of generalised surveillance of people's internet activity by states, as well as by private actors on states' behalves, that we have never seen before in a democratic society. It would force companies to subject their users to mass scanning, basing this on an assessment of the general risk profile of a platform or service, rather than warranted, individualised suspicion in accordance with the rule of law.[3] And in the case of encrypted services or platforms, it would force them to use scanning technologies that amount to spyware. Furthermore, it is likely to make investigations into child sexual abuse (CSA) slower and less likely to lead to convictions; and runs a high risk of criminalising the sexual expression of adolescents and LGBTQI+ individuals, therefore also infringing on the rights to freedom of expression and non-discrimination (see response to question 3).

Going deeper into the core fundamental rights question, under Article 52 of the EU Charter of Fundamental Rights, any restriction on fundamental rights must be demonstrably necessary and proportionate, and with sufficient safeguards. For example, if police reasonably suspect someone of child sexual abuse, and as long as they follow due process, it is legitimate for them to limit the privacy, data protection and certain other rights of that suspect.

The European Commission does not dispute that the proposed EU Child Sexual Abuse Regulation contains intrusive measures which would constitute an interference with fundamental rights including the rights to privacy, data protection and free expression of internet users. So the key question is whether the proposed level of interference with these fundamental rights can be justified or not. The seriousness of the crime of CSA and the obligation to protect children are very important. Under EU law, however, even serious crimes do not mean that states can take any measure at any cost.

There are several ways to assess these measures. Firstly, in order to demonstrate that the proposed law is necessary and proportionate, there must be no less intrusive option possible. As will be explained in my response to question 3, there are many less intrusive options that could be pursued by the EU. Secondly, the effectiveness and efficiency of the proposed measures must be backed up by objective evidence, which is missing from the Commission's impact assessment.

Thirdly, the fundamental rights balancing test must show that the infringement of rights is proportionate and not excessively harmful. EDRi's analysis demonstrates that the proposal would seriously interfere with the fundamental rights of potentially all internet users, depriving them of critical digital security and privacy which is essential for the realisation of a wide range of their economic, social, cultural and political rights. This is the case regardless of whether they are suspected of grooming or disseminating child sexual abuse material (CSAM), or if they are are only using the internet for legitimate and lawful reasons (as most internet users are). That's because there is no way to genuinely target Detection Orders.

3 We explain what fundamental rights and rule of law-compliant investigations into CSA look like. EDRi, '10 principles to defend children in the digital age', 09 February 2022, available at: https://edri.org/our-work/chat-control-10-principles-to-defend-children-in-the-digital-age/.

As a result, the Commission has failed in its burden of proof to justify the necessity and proportionality of the restriction on fundamental rights by the proposed CSA Regulation. This is a critical part of EU lawmaking, and it is harmful to our shared EU values for the Commission to put forward a proposal with so many gaps in this regard. This underpins EDRi's call for the co-legislators to reject the proposal, and call on the European Commission to produce a draft law which is compliant with EU law and which does justice to the importance of tackling CSA. Our recommendation that the Commission withdraws the law is supported by 123 other civil society groups, including children's digital rights, women and girls' empowerment, victim support, lawyers, open software, media freedom and digital rights organisations.[4]

2. The Commission's proposal provides for the issuance of detection orders requiring providers of communications services or devices to covertly access information if it is suspected that abuse material is being shared via these services or devices or that grooming is taking place on them. In your view, what services and devices are potentially affected by this and to what extent, and what effects will this have on their users.

The providers in the scope of Detection Orders are any 'provider of hosting services' or 'interpersonal communications services' operating in the EU (Article 7(1)). These terms are defined broadly, including social media platforms, message boards / chat sites, gaming websites with chat functions, cloud services providers, file sharing services, messaging apps, dating apps and so forth. Because of the wide scope, the only exclusions would be for an individual entirely self-hosting and self-running a service (e.g. a person operating their own email service and server for completely personal use), whereas a person hosting an email server and service for their work, or as a free open-source project, would be in the scope of the rules. We foresee a potentially very large impact on small providers as well as free and open source software (sometimes called FOSS / FLOSS) providers who will be expected to comply with the same rules as big tech. This could lead to a further concentration of power for big tech providers who are more easily able to comply. This could also disincentivise the creation and use of FOSS/FLOSS.

The impacts upon users will be very wide ranging, but to give one example: an encrypted message service could be forced under Articles 7-11 (Detection Orders) to either scan their users' messages (which would inevitably mean using 'Client Side Scanning'), to abandon the encryption that they have promised their users, or to leave the EU market. WhatsApp and Signal have both spoken on the record about leaving jurisdictions where their use of encryption would be compromised. The result is that Europeans could be left without access to secure and private message services – putting journalists, whistleblowers, human rights defenders, politicians, people seeking healthcare, religious communities, LGBTQI+ communities, victims of domestic violence / intimate partner violence (including stalking, which frequently has a digital component) and minoritised communities at particular risk.

4 EDRi, 'European Commission must uphold privacy, security and free expression by withdrawing new law, say civil society', 08 June 2022, available at: https://edri.org/our-work/european-commission-must-uphold-privacy-security-and-free-expression-by-withdrawing-new-law/.

3. Why, in your opinion, is the Commission's proposal fit for purpose or not fit for purpose when it comes to protecting children effectively from (sexual) abuse and the dissemination of abuse material, and where do you believe concrete action is needed?

Regrettably, there are several reasons why the Commission's proposal is not fit for purpose for protecting children from sexual abuse, and in fact may make the fight against CSAM harder:

1. Currently, over 90% of CSAM is removed from the internet by child protection hotlines (the German hotline is called eco) within a couple of days. Child rights and child protection groups are unanimous that the fast removal of CSAM from the internet once it has been identified is the top priority to protect survivors. However, the proposed CSA Regulation sets up a complex and bureaucratic system of reporting and responses which will take several months to act on content removals or suspicion of grooming. This extended time period will not only mean that victims are left waiting and at risk, but also that when the reports are finally acted upon, the original data are likely to have been deleted already, due to data retention rules. This is likely to make convictions against perpetrators harder to secure;
2. The proposal additionally does not give any formal role to the hotlines, which currently perform vital child protection work despite receiving only precarious funding and in many member states, operating with only a handful of staff. As I will explain in several subsequent questions, the proposed role of the EU Center seems to overshadow the vital role of these hotlines, instead of supporting their critical work;
3. As explained in more detail in my response to question 4, it is likely that false reports will clog up the entire system (like searching for a needle in a haystack), meaning that there is less attention and resources available for real cases of CSA, and significant amounts of time wasted investigating false cases;
4. We are also concerned that the sexual self-expression of adolescents will be criminalised under the proposal. In six EU Member States, it is lawful for adolescents of a certain age to consensually share intimate material (e.g. nude selfies, sexts). However, under the CSA Regulation, such content – despite being lawful at a national level – would be considered CSAM. If flagged by a provider, it would have to be reviewed by a moderator, then be sent to the EU Center, and then on to national law enforcement to investigate. This means that adolescent's consensual and lawful intimate images could be routinely shared with multiple individuals, and young people subject to investigations simply for exploring their sexual self identity. The risk is especially high for LGBTQI+ young people, who often rely heavily on digital tools for sexual self expression. In countries where LGBTQI+ face systemic discrimination, the risks posed to queer people by revealing their sexual activity and expression can be a matter of physical safety;
5. As explained in more detail in question 9, the generalised monitoring of young people's digital activities can be very harmful for their development and free expression, and deprive them of safe online spaces and even ways to seek help when suffering abuse;
6. Sex education is also likely to be impacted by the proposed grooming detection. Swedish sexual education and reproductive rights charity, RFSU, told us that it is

common for important sexual health information to be shared via encrypted messages, especially in places where young people do not have good access to such education. The CSA Regulation's proposed grooming detection would be likely to flag any adult providing sexual education or information about LGBTQI+ issues to an adolescent as a perpetrator of CSA, which could lead to a severe chilling effect on sexual education.

The severity and volume of these risks to the fight against CSA and harms to young people and adults alike lead EDRi to conclude that amendments will not be sufficient to make this proposal a) effective nor b) fundamental rights compliant. We strongly suggest that Member States pursue the wide range of alternative options already at their disposal and in many cases, much more quickly implementable than the proposed legislation, for example:

- The implementation of the recently-adopted Digital Services Act, which was agreed be European co-legislators to tackle all forms of illegal material online, including CSAM. In particular, the new notice-and-action mechanism and system of trusted flaggers will have a positive impact on the removal of CSAM from the internet;
- The reform of the 2011 EU Child Sexual Abuse Directive, a law designed to tackle child sexual abuse in EU member states, the implementation of which has been so poor that the European Commission has had to launch infringement proceedings against several non-compliant member states;
- Investment in the national hotlines, as previously discussed in this question;
- 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;
- Pursuing ambitious social reforms, often at national level, including around welfare, anti-poverty measures, social services, police reform and judicial reform;
- 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 US Centers for Disease Control and Prevention (CDC) explains that many effective or at least promising prevention strategies are known about, but are hardly tested or implemented around the world.[5]

4. How great is the risk, in your view, of innocent members of the public coming under suspicion due to false positives produced by automated detection, and what would the impact of such false positives be for both the suspects and the investigating authorities?

5 CDC, 'Fast Facts: Preventing Child Sexual Abuse', 6 April 2022, available at: https://www.cdc.gov/violenceprevention/childsexualabuse/fastfact.html.

False alerts and their consequences are very harmful. An investigation by EDRi members ICCL and DRI in Ireland has shown that at least 10% of the CSAM reports received by the Irish police were false alerts, and the real number is likely to be much, much higher.[6] Of these reports, hundreds were confirmed to be legitimate activities: including consensual intimate content shared by adults; and families playing on the beach or in the bath.

Despite confirming the innocence of the individuals involved, the Irish police held onto the personal data of these persons. This is currently being investigated but is likely to amount to unlawful data retention. The consequences of false alerts can range from people being locked out of their digital lives (e.g. permanently losing access to all their photos and email accounts) and wrongfully investigated by police, to people losing their children, their jobs, and taking their lives.

The proposal relies on artificial intelligence (AI) based 'indicators' to detect new CSAM and grooming. These indicators may be able with some level of accuracy to detect features like nude skin, or an estimated age bracket for a person, but this is not the same as detecting CSAM. For example, a very high number of photos and videos containing nude skin that are exchanged online are lawful and legitimate. AI systems do not have common sense and will never reliably be able to distinguish between legitimate content and CSAM. This means that a very high number of false alarms are inevitable.

The system established by the CSA Regulation nevertheless requires all alerts to be sent firstly to the EU Center, and then on to national law enforcement, unless they are "manifestly unfounded" as CSAM (for example, an erroneous picture of a dog, which no-one could consider to be CSAM). In some Member States, the police are obligated to investigate these reports. Already under-resourced police forces in Germany and the Netherlands have said that they would not be able to deal with the huge volume of false reports that they would receive under this proposal.[7]

5. According to Article 10 of the draft CSAM Regulation, providers of hosting services and providers of interpersonal communications services that have received a detection order are to install and operate technologies to detect the solicitation of children with abusive intentions ("grooming"). Are you aware of technologies that can reliably distinguish between unobjectionable sexual or romantic communication and grooming?

No, I am not aware of any technologies that can reliably do so. Grooming is difficult for experienced social workers and police officers to detect, and convictions for grooming are low as a result of the difficulty to prove grooming.

6 EDRi, 'A Safe Internet for All', October 2022, available at: https://edri.org/wp-content/uploads/2022/10/EDRi-Position-Paper-CSAR.pdf, page. 53.

7 Tweede Kamer, 'Europese Verordening ter voorkoming en bestrijding van seksueel kindermisbruik', 04 October 2022, available at: https://debatgemist.tweedekamer.nl/node/29579 and Deutschland Funk,'Sexueller Kindesmissbrauch: Wie Ermittler im Internet vorgehen', 20 October 2022, available at: https://www.deutschlandfunk.de/strafverfolgung-sexueller-kindesmissbrauch-datenschutz-100.html.

6. What technical approaches do you believe offer effective, rights-compliant alternatives to the measures set out in the draft Regulation?

We often hear from developers and deployers of technology that their systems or methods can provide the answer to complex societal problems. The reality is of course a lot more nuanced, and technological approaches will – at best – be a small puzzle piece in a much larger set of approaches which focus on educational, societal, police and judicial reform.

The places where technology can provide an assistive role are generally the simpler alternatives: as discussed in question 3, an obligation on providers to have an easily-accessible and child-friendly reporting button is one simple but powerful idea.

Other ideas around user empowerment and control could also be explored, which would fit the recommendation from Child Rights International Network (CRIN) that the best way to keep young people safe online is to ensure that they are properly educated, that they feel empowered in online spaces (rather than surveilled or afraid, which does not lead to sensible behaviours) and that they have trusted adults that they can turn to when something doesn't feel right.

There have also been promising investigations into non-mass-surveillance methods of child protection in online environments, such as the 'Fortnite Undercover Avatar' project by child protection group L'Enfant Bleu in collaboration with the French police.[8] This project was designed to use creative methods to bring 'traditional' police investigatory work and child psychologists into digital spaces, and was successful in supporting 1.200 at-risk children in a period of less than two months. 400 of these children were subsequently found to be at "dire" risk of abuse. The project was suspended due to a lack of resource, but it shows what can be achieved if we invest time and funding into the right areas.

7. The Commission's proposal includes a call for mandatory age verification. Where exactly,and in what circumstances, would internet users have to verify their age under this proposal, and what technical options exist or are currently being explored to implement age verification in a rights-compliant manner that preserves the anonymity of users online?

Articles 3 and 4 require the use of age verification for social media, cloud, email, chat/message and other hosting and interpersonal services providers that have identified a risk of grooming on their platform. The wording of the proposal is such that any provider that does not employ age verification is likely to be considered risky in effect mandating widespread age verification. If a provider cannot show that they have reduced the risk to almost zero, then they could be subject to a Detection Order, and subsequently a fine of up to 6% of their turnover.

We are not aware of any age verification methods which preserve anonymity of users and are rights-compliant. All of the methods of which we are currently aware come with risks to privacy and data protection posing a particular risk to people whose work, safety, and/or

8 Europol, 'Europol Excellence Award in Innovation', undated, available at: https://www.europol.europa.eu/media-press/newsroom/news/europol-excellence-award-in-innovation.

participation in democratic life relies on anonymity online. Several known methods also have a high risk of exacerbating the digital exclusion of already vulnerable communities, particularly of undocumented people, Roma and Sinti communities, and elderly people – effectively blocking their access to digital services.

8. The Commission's proposal would make it possible for private communications services to be required to comply with detection orders, including to obtain content from private and encrypted chats (for example through client-side scanning) to detect grooming or for the purpose of age verification; the technology-neutral approach means that access blocking is potentially also conceivable. What would the international consequences be of such means of analysing user behaviour or restricting access to online content and safe spaces – especially regarding the higher risk of illegal foreign encroachments on European citizens' privacy (hacking), and regarding authoritarian regimes' use of the EU rules as a blueprint for illegitimate surveillance measures that are not constrained by the rule of law?

I would like to note that the Commission's proposal is not technologically neutral; it is very clearly foreseeable that it will impact encryption, and that to do so, providers will have no choice but to use 'Client Side Scanning' (CSS). That's because in order to access the content of an encrypted message, some sort of entry has to be created into the message.

CSS has never been successfully deployed at scale, and the European Commission's expert group, who were appointed to assess various methods of CSS, found a combination of low and medium feasibility, privacy and security in even their top three methods of CSS (this can be seen in the impact assessment). Given that the impact assessment is supposed to demonstrate the effectiveness of the proposal, it is very problematic that these conclusions have been repeatedly misrepresented.

Added to this, there has been an outcry from cybersecurity, technology and privacy professionals around the world, who have all confirmed that CSS cannot be done safely, securely and in a manner that respects fundamental rights.

What's more, once CSS has been implemented on someone's device, it is like creating a back door which anyone can enter: stalkers, malicious states, hackers, child abusers, or any other mal actors. It would be bizarre to say the least for the bloc that created the GDPR, and which is currently developing rules to improve cybersecurity, to usher in an unprecedented mass surveillance law which would weaken privacy and security of the entire internet ecosystem.

9. The Child Rights International Network recently underlined in a study the importance of "mov[ing] beyond a privacy versus protection framing if we are to ensure that all children's rights are protected". What approach does the European Commission's current proposal take to the right of children and young people to privacy and secure IT systems, and what short-term and long-term consequences would the Commission's proposal have in this context?

The Commission's proposal thoroughly analyses children's right to be free from sexual abuse and exploitation, but does not consider or assess their rights to self-expression, informational self-determination (access to information) or autonomy online. Under the Commission's proposal, the internet is presented as a very dangerous place for under-18s, and nothing more, meaning that the fundamental rights balancing test performed by the Commission in the impact assessment is inadequate. This inadequacy has been recognised by the European Parliament, who have commissioned an independent consultant to re-do parts of the Commission's impact assessment in order to better consider all of the fundamental rights risks at play.

In the proposal, there is no recognition of young people as legitimate internet users, nor the value of digital communications and communities for seeking support (especially victim support and mental health support) and for developing their autonomy. Both UNICEF and the UN have emphasised the importance of digital spaces for young people, and warned against measures that would constitute generalised surveillance of their internet use.[9] And as CSA survivor Alexander Hanff explains, surveilling survivors' conversations can disempower them and ultimately discourage them from coming forward to report their abuse.[10]

10. In your view, what package of political measures would, taken together, offer a promising approach to tackling sexual violence against children in an effective and rights-compliant manner? Where is there potential for adjustments and improvements in the field of prevention and in tackling sexual violence and online material depicting it?

Even if we were to put to one side all of our concerns about the proposed CSA Regulation, a 'perfectly functioning' CSA Regulation would still not mean that CSA is no longer happening. It is a proposal which looks to tackle one of the symptoms of the heinous crime of CSA (in this case the role of online intermediaries in the dissemination of CSAM and grooming), without addressing the vicious societal roots of the issue. That's why the only truly effective measures are prevention – as that's what stops children from being harmed in the first place. For the most part, the CSA Regulation only acts once the abuse has been committed. This also points to the problem of the legal basis of the proposed CSA Regulation, which is the harmonisation of the single market. By using this basis, the EU is presenting solution to the dissemination of CSAM as an economic and business problem, rather than a societal one.

We have performed a wide review of literature on child abuse prevention recommendations, which is what underpins the recommendations made in question 3. In the interest of space, full references and results of literature review are available on request.

9 United Nations, 'General comment No. 25 (2021) on children's rights in relation to the digitial environment', 2021, available at: https://digitallibrary.un.org/record/3906061?ln=en and UNICEF, 'Children's online privacy and freedom of expression toolkit', May 2018, available at: https://sites.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf.

10 Alexander Hanff, 'Why I don't support privacy invasive measures to tackle child abuse', 11 November 2020, available at: https://www.linkedin.com/pulse/why-i-dont-support-privacy-invasive-measures-tackle-child-hanff.

11. Does the European Commission's proposal effectively cover all online platforms on which child pornography material can be disseminated, and if not, what kind of improvements are potentially needed regarding the proposal's scope of application?

To the contrary, the scope of the proposal is very broad. It includes not just the typical social media companies and apps that we might think of, but also emails, cloud infrastructure providers, providers of phone call and text message services, and even individuals running a small server, for example on behalf of their work colleagues. If the obligations on providers were reasonable, then this broad scope might not be such a problem (it would be reasonable to expect all providers to take reasonable steps and measures to reduce the risk of CSA on their platform or service). However, the proposed measures are not reasonable, meaning that the broad scope is very problematic.

12. Does the European Commission's proposal give sufficient consideration to instruments to improve prosecution and enforcement? Where are improvements potentially needed, and what instruments would be necessary for this purpose?

No it does not. There is an urgent need for improvements in prosecution and enforcement which would be better tackled at member state level. In particular, judicial and police reform is needed, and should be undertaken from a trauma-informed and survivor-focused perspective. This means starting with a survivor's perspective of what justice looks like and how to achieve it, including consulting with survivors, as well as all other relevant stakeholders in accordance with their expertise. See question 3 for more information about the DSA and 2011 Child Sexual Abuse Directive, which can support national efforts.

13. Will the new EU Centre be able to adequately support national law enforcement agencies and Europol, according to the current plans, and what resources would it require to do so?

I do not believe that the EU Center will be able to adequately support national law enforcement agencies. Whilst an EU Center in principle is not problematic, its scope should be dramatically narrowed, and re-focused on education, prevention, and on supporting hotlines to carry out the frontline work (see question 3). It should be entirely independent from Europol.

14. In your opinion, does the European Commission's proposal encompass all technical approaches which can be used to achieve the aim of protecting children, and what other technical approaches would be necessary, in your view?

Technological approaches will always be inherently limited. I recommend that 'low' tech measures (e.g. mandatory reporting buttons, user control functionalities) are investigated before considering more intrusive technologies, and that societal – in particular preventative – measures are always given precedence. With child protection groups confirming that 80-90% of CSA is committed by someone known to the victim, the benefits of systematic criminal record checks, of earlier police intervention (e.g. believing survivors when they come

forward, which has been recorded as a systematic problem) and other non-technical measures are clear.

15. The draft Regulation also provides for the possibility of blocking access to individual URLs, and changes to the proposal during the Czech Presidency of the Council even seek to further expand this possibility. Given the widespread use of https encryption for URL requests, do you believe it is technically feasible to specifically block individual URLs without resorting to blocking entire domains? If so, how is this possible, and if not, can this kind of access blocking comply with the requirements established by the European Court of Justice as regards the targeting of access blocking?

No, our assessment is that the widespread use of https means that to implement a blocking order, internet access providers will be forced to block entire domains. For example, to block one page on Wikipedia because of suspected CSAM, the entirety of Wikipedia would have to be blocked. This would not comply with requirements for targeted blocking.

16. What is your view of the role and nature of the planned EU Centre envisaged by the draft EU Regulation, firstly with regard to the performance of primarily preventive tasks, and secondly with regard to tasks relating to the development and use of technical surveillance tools?

Very little information is provided about the preventative tasks of the EU Center. However, the whole CSA Regulation is presented as a preventative legislation, which is not in line with the methods or models of the proposal. The EU Center's development and use of technical surveillance tools will always be problematic in the context of a Regulation which encourages the use of dangerous tools. Hypothetically, if a coordinated EU child protection entity were to have a role over the use of child protection technologies, it would be critical for there to be oversight from the European Data Protection Board as well as from independent privacy and security experts. There would also need to be a high level of transparency.

17. If scanning targeted the communications taking place on devices ("chats"), rather than the devices themselves, the same issues would exist regarding the end-to-end encryption of messaging services, for example. Again, countless law-abiding citizens would end up in the sights of the authorities simply because of their use of a specific service and the corresponding software. Are you aware of software solutions that allow end-to-end encrypted communications to be read in real time or at least decrypted? Do you believe it is justifiable to use algorithms to break the confidentiality of private communications, which is guaranteed by the German constitution?

By nature, any software 'solution' that reads encrypted communications in real-time, or decrypts them, by definition is violating the fundamental purpose and essence of the end-to-end encryption. It is equivalent to going into someone's house to read a letter over their shoulder while they are writing it, and claiming that it is acceptable because you didn't open

the envelope. It is still an unacceptable violation of privacy (unless there is reasonable, individual suspicion against them) and that is not something that any amount of technological development can change.

Whether by algorithm or other methods, it is only justifiable to break the confidentiality of private communications in the event that there is reasonable suspicion of a crime serious enough to warrant that intrusion. This is not just constitutional, but also set by the EU Charter of Fundamental Rights and enforced by the CJEU.

18. The draft Regulation states that the EU Centre on Child Sexual Abuse to be established in The Hague is to generate binding indicators of sexual abuse material, which are to be used by the companies carrying out the scanning. Yet experienced investigators know that it is impossible to unequivocally define and substantiate on a case-by-case basis what criteria determine what constitutes a family photo, a self-documented game among children and young people, a chance snapshot of a sporting event, or, indeed, child pornography. Is any information already available about the methodology used by the EU Centre? And if so, can this methodology be regarded as reliable and suitable?

I fully agree; see my response to question 3 for more information about the inability of AI-based tools to make such differentiations. Limited information is available about how the Commission foresees this, however Felix Reda's 2022 freedom of information request confirmed that the Commission relied on un-vetted claims made by technology providers about the functioning of their technologies.[11] Based on the Impact Assessment accompanying the Commission's proposal, I think it is likely that the Commission plans for the EU Center to use software from Thorn / Safer. Thorn is a not-for-profit organisation which provides free-of-charge scanning technology from US-based commercial scanning technology company Safer. Both Thorn and Safer are led by Ashton Kutcher.[12]

For more information, please contact: Ella.Jakubowska@edri.org

11 See Ask The EU, 'technologies for the detection of new CSAM referenced by Commissioner Johansson', starting from 08 August 2022, available at: https://www.asktheeu.org/en/request/technologies_for_the_detection_o.

12 Netzpolitik.org, 'Dude, where's my privacy? How a Hollywood star lobbies the EU for more surveillance', 12 May 2022, available at: https://netzpolitik.org/2022/dude-wheres-my-privacy-how-a-hollywood-star-lobbies-the-eu-for-more-surveillance/.