A Critical Analysis in the EU's CSAM Proposal.

Assessing the Proposal's suitability under Article 5(4) of the Treaty on the Functioning of the European Union, in light of current detection technologies and ease of circumvention.

Alexander Hanff

31st August 2023

Contents

Introduction....3
1. Opposition against the Proposal....6
1.1 The situation outside the European Union....9
1.2 Potential to challenge the Proposal before the CJEU....11
2. Suitability....13
2.1 Challenges related to the high number of reported material....13
2.2 Technological Shortcomings....16
2.3 Risks arising from the emergence of Generative Artificial Intelligence....18
2.4 Policy considerations on synthetic CSAM and deep fakes....19
3. Problems related to criminalising behaviour, lack of evidence based data and risk of circumvention....21
3.1 Criminalising consensual sexual conduct....21
3.2 Problems of evidence-based numbers put forward in the Proposal....21
3.4 Challenges related to the dark web....23
3.5 Understanding communications networks....25
3.6 The use of VPNs and additional private networks and similar....26
4. Conclusion....29
Personal Testimony....32
Bibliography....36

Introduction

In July 2021, the European Parliament and Council of Ministers respectively, adopted a proposed derogation (the Derogation)[1] to Directive 2002/58/EC (ePrivacy Directive)[2] in relation to the confidentiality of communications for the purpose of the detection of Child Sexual Abuse Media (CSAM).

The ePrivacy Directive aims at ensuring the confidentiality of communications (Article 5) in accordance with Article 7 of the Charter of Fundamental Rights of the European Union (EU Charter)[3], by strictly limiting how communications data which traverses a public telecommunications network may be processed.

As a general rule, it is unlawful to process such data without consent, other than for the conveyance of communications over a public telecommunications network, with limited interference permitted by Member States in order to detect and prevent national security threats and serious crime as deemed as a "necessary, appropriate and proportionate measure within a democratic society." (Article 15(1)).

The Derogation introduced temporary measures to allow technology platforms facilitating interpersonal communications between individuals and groups, to scan the communications of the users of their platforms in order to detect, report and remove CSAM (Article 3).

Several platforms had already been scanning interpersonal communications (with a technology known as PhotoDNA[4]) for some time, which had arguably been lawful as these platforms were not within the scope of the ePrivacy Directive.

However, amendments to the European Electronic Communications Code (EECC) in 2018 (which came into effect in December 2020), broadened the definition of an 'electronic communications service' to include 'interpersonal communications service' otherwise known as 'over the top' or 'ott' service "that enables 'direct interpersonal and inter-

[1] European Commission Proposal 2020/0259 (COD). (https://eur-lex.europa.eu, 9 October 2020) <https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2020/0568/COM_COM(2020)0568_EN.pdf> accessed on 14 June 2022.

[2] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L201/37.

[3] Charter of Fundamental Rights of the European Union [2012] OJ C326/391

[4] Microsoft Inc., 'PhotoDNA' (https://www.microsoft.com, date unknown) <https://www.microsoft.com/en-us/photodna> accessed 12 August 2023.

active exchange of information via electronic communications networks between a finite number of persons'"[5].

This change in law brought online services such as Social Media (SoMe) platforms into scope of Article 5 of the ePrivacy Directive, creating significant concerns that the scanning of communications for the detection of CSAM would become unlawful.

The adopted proposal became law on 14 July 2021 but the final version had a limited sunset[6] which created urgency to propose a more permanent solution before ceasing of its effect. This would meet the commitment by the European Commission (EU Commission) in their explanatory memorandum, to introduce a long-term solution.[7]

To this goal, in May 2022 the EU Commission published a new proposal[8] (the Proposal) which would be a permanent replacement to the Derogation and make the above described activities a mandatory requirement on all 'relevant information society services'[9] - whereas under the derogation such activities were voluntary.

Further, the Proposal would require all such service providers to conduct a risk assessment (Article 3), mitigate any risks found (Article 4) and risk reporting (Article 5) as well as adherence to 'detection orders' (Article 7) and would include detection of not just known CSAM but also new CSAM and so called grooming.

Rather than focusing on the various legal obligations presented in the Proposal (repeating work already published[10]) the aim of this thesis is to consider the legal issues the Proposal faces in relation to the EU Treaties and the EU Charter. This thesis will particularly focus on the suitability of the proposed solutions, current practices and future threats posed by the rapid emergence of synthetic media produced by generative artificial intelli-

[5] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast)Text with EEA relevance. [2018] OJ L321/36.

[6] 3rd August 2024 vs 31st December 2025

[7] "This proposal respects the fundamental rights, including the rights to privacy and protection of personal data, while enabling providers of number-independent interpersonal communications services to continue using specific technologies and continue their current activities to the extent necessary to detect and report child sexual abuse online and remove child sexual abuse material on their services, pending the adoption of the announced long-term legislation." (Section 1 - Context of the Proposal).

[8] European Commission Proposal 2022/0155 (COD). (https://eur-lex.europa.eu, 11 May 2022) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN&qid=1652451192472> accessed 14 June 2022.

[9] Defined in Article 2 as hosting services, interpersonal communications services, software application stores and internet access services.

[10] Dr. Teresa Quintel, 'The Commission Proposal on Combatting Child Sexual Abuse - Confidentiality of Communications at Risk?' (2022), European Data Protection Law Review 262.

gence (GenAI). Furthermore, it will point to potential consequences in relation to research, support services and false positives.

1. Opposition against the Proposal

While having been praised by several child organisations[11] and law enforcement the current Proposal has come under attack by various Non Governmental Organisations (NGOs)[12], Parliamentarians[13], Legal Scholars[14] and others[15], on the basis that such activities pose a significant risk to the the fundamental right to privacy under Article 7 of the EU Charter.

Indeed, just two days prior to the EU Commission publishing their proposal for a permanent Regulation, German MEP Patrick Breyer filed a lawsuit against Meta Platforms Ireland Limited in the Kiel District Court[16].

The complaint seeks an injunction against the use of the Derogation for "the suspicionless automated search of private chat histories and photos"[17] in the 'Facebook Messenger' software application.

Breyer's case would seem to be supported by a legal opinion[18] commissioned from a former Judge of the Court of Justice of the European Union (CJEU)[19], which concluded:

[11] Internet Watch Foundation, 'Draft report on vital EU proposal to stop child sexual abuse welcomed as 'strong and balanced' (https://iwf.org.uk, 9 May 2023) <https://www.iwf.org.uk/news-media/news/draft-report-on-vital-eu-proposal-to-stop-child-sexual-abuse-welcomed-as-strong-and-balanced/> accessed 28 August 2023.

[12] European Digital Rights Initiative, 'Private and secure communications attacked by European Commission's latest proposal' (https://edri.org, 11 May 2023) <https://edri.org/our-work/private-and-secure-communications-put-at-risk-by-european-commissions-latest-proposal/> accessed 9 August 2023.

[13] Patrick Breyer MEP, 'Chat Control: The EU's CSEM scanner proposal' (https://patrick-breyer.de, date unknown) <https://www.patrick-breyer.de/en/posts/chat-control/> accessed 17 August 2023.

[14] German Bundestag Research Services, '"Chat control" - Analysis of the EU Commission's draft regulation 2022/0155 (COD)(English translation)' (https://patrick-breyer.de, 7 October 2022) <https://www.patrick-breyer.de/wp-content/uploads/2022/10/221007-WD-10-026-22-Bewertende-Analyse-zur-Chatkontrolle_EN-1.pdf> accessed 7 August 2023.

[15] European Parliamentary Research Service, "Proposal for a regulation laying down the rules to prevent and combat child sexual abuse - Complimentary impact assessment" (https://europarl.europa.eu, April 2023) <https://www.europarl.europa.eu/RegData/etudes/STUD/2023/740248/EPRS_STU(2023)740248_EN.pdf> access 19 August 2023.

[16] Steinmeier, '20220509_Unterlassungsklage_Facebook_Breyer' (https://patrick-breyer.de, 9 May 2022) < https://www.patrick-breyer.de/wp-content/uploads/2022/05/20220509_Unterlassungsklage_Facebook_Breyer.pdf> accessed 17 July 2023.

[17] Patrick Breyer MEP, '"Destruction of digital privacy of correspondence": lawsuit filed against chat control' (https://patrick-breyer.de, 10 May 2022) <https://www.patrick-breyer.de/en/destruction-of-digital-privacy-of-correspondence-lawsuit-filed-against-chat-control/> accessed 29 July 2023.

[18] Prof. Dr. Ninon Colneric, 'Legal opinion commissioned by MEP Patrick Breyer, The Greens/EFA Group in the European Parliament' (https://patrick-breyer.de, March 2021) <https://www.patrick-breyer.de/wp-content/uploads/2021/03/Legal-Opinion-Screening-for-child-pornography-2021-03-04.pdf> accessed 13 March 2023.

[19] Commissioned by Patrick Breyer MEP and The Greens/EFA Group in the European Parliament

"EU legislation obliging providers of number independent communications services (i.e. e-mail, messaging, chat) to generally and indiscriminately screen the content of all private correspondence for 'child pornography' and report hits to the police would not comply with the fundamental rights guaranteed by Articles 7, 8, 11 and 16 of the Charter." [20].

Further, a YouGov poll from March 2021 illustrated that less than 20% of over 10 000 participants approved of rules that would allow the indiscriminate scanning of emails without suspicion; with 72% of respondents stating '"I am against personal electronic mail and messages being searched without suspicion."' The poll showed no significant variance between different genders or age groups[21].

This seems contrary to a Eurobarometer poll[22] commissioned by the EU Commission if one is to only read the 'Key Findings', but a more diligent reading of the questions in the poll tells a different story.

For example - at no point does the Eurobarometer poll mention that the Proposal would require the interception and reading of all digital communications but instead relies on questions which seem designed to trigger an emotional response rather than an informed and rational one.[23]

However, it is not only polls and commissioned reports that oppose the Proposal. In July 2022 the European Data Protection Board (EDPB) and the European Data Protection Supervisory (EDPS) published a joint opinion[24] criticising the Proposal on multiple fronts including '"proportionality of the envisaged interference and limitations to the protection

[20] ibid, p 34.

[21] YouGov, 'Omnibus International - Topic: Chat Control - 10 countries' (https://nextcloud.pp-eu.eu, April 2021) <https://nextcloud.pp-eu.eu/index.php/s/5bkdRGyxnAciNBz?dir=undefined&openfile=372951> accessed 14 March 2023.

[22] Eurobarometer, 'Protection of children against online sexual abuse.' (https://europa.eu, July 2023) <https://europa.eu/eurobarometer/surveys/detail/2656> accessed 30 August 2023.

[23] Eurobarometer, 'Protection of children against online sexual abuse - data annex' (https://europa.eu, July 2023) <https://europa.eu/eurobarometer/api/deliverable/download/file?deliverableId=88194> accessed 30 August 2023.

[24] European Data Protection Board and European Data Protection Supervisor, 'Joint Opinion 4/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse' (https://edps.europa.ee, 28 July 2022) <https://edps.europa.eu/system/files/2022-07/22-07-28_edpb-edps-joint-opinion-csam_en.pdf> accessed 17 June 2023.

of the fundamental rights to privacy and the protection of personal data."'[25], a lack of "clarity on key elements"[26] and "legal uncertainty"[27].

Additional issues raised by the Opinion such as the interference with end to end encryption (e2ee)[28] in order to facilitate the use of 'detection orders' in encrypted messenger software applications (such as Signal, Telegram, WhatsApp etc.) are echoed by NGOs, politicians, academics and privacy advocates[29].

[25] ibid, p 16-23.

[26] ibid, p 5.

[27] ibid, p 13-15.

[28] ibid, p 27.

[29] Callum Voge, 'EU's contempt for encryption puts all Europeans at risk" (https://euractiv.com, 21 September 2022) <https://www.euractiv.com/section/digital/opinion/eus-contempt-for-encryption-puts-all-europeans-at-risk/> accessed 19 June 2023.

1.1 The situation outside the European Union

In an attempt to bypass concerns related the EU Commission's published strategy to introduce a long-term replacement to the Derogation[30], Apple Inc. introduced new tools to help them detect CSAM material on their platforms including their iCloud platform which is used to backup photos and various other data by Apple's customers[31].

The new tools avoided issues relating to interference with e2ee by scanning images that were to be uploaded to users' iCloud storage prior to being encrypted; but the news backfired dramatically on the World's most valuable technology company.

Despite Apple's intent to provide a solution which would not interfere with e2ee and would be based on the principles of 'privacy by design'[32] the announcement led to the publishing of an open letter signed by almost 10 000 security and privacy experts to 'Decry Apple's Planned Move to Undermine User Privacy and End-to-End Encryption'[33].

The signatories argued that the plan undermined e2ee and would open the door for other sovereign nations to impose requirements on Apple to scan for other content such as political speech or content in relation to non-heterosexual activity. Oddly enough, this author notes that no more than a handful of these signatories protested the Derogation which was adopted by the EU just a few weeks prior to Apple's announcement.

It is important to note that in the United States under the Communications Decency Act (CDA) signed into law by President Bill Clinton in 1996, online platforms are generally immune from prosecution for hosting CSAM on their platforms under §230[34] of the US Code, if they are unaware of such - an immunity which was upheld in a recent

[30] European Commission, 'Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions' (https://eur-lex.europa.eu, 24 July 2020) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0605> accessed 7 August 2023.

[31] Apple Inc., 'Expanded Protections for Children' (https://apple.com, 5 August 2021) <https://www.apple.com/child-safety/> accessed 22 August 2023.

[32] Information Privacy Commissioner of Ontario, 'Privacy by Design' (https://ipc.on.ca, January 2018) <https://www.ipc.on.ca/wp-content/uploads/2018/01/pbd-1.pdf> accessed 3 February 2023.

[33] Author unattributed, 'An Open Letter Against Apple's Privacy-Invasive Content Scanning Technology' (https://appleprivacyletter.com, 6 August 2021) <https://appleprivacyletter.com/> accessed 22 August 2023.

[34] Cornell Law School, '47 U.S. Code § 230 - Protection for private blocking and screening of offensive material' (https://law.cornell.edu, date unknown) <https://www.law.cornell.edu/uscode/text/47/230> accessed 20 August 2023.

Supreme Court ruling[35] which denied a petition to bring the matter before the Court, further strengthening immunity under §230 of the CDA.

This particular cases attempted to use a new exemption to §230 of the CDA signed into law in 2018 by President Donald Trump under the 'Allow States and Victims to Fight Online Sex Trafficking Act' (FOSTA)[36]. Jane Does No. 1-6 et al. argued that Reddit, Inc was facilitating criminal sex trafficking of children by failing to remove reposts of CSAM which they had previously removed, but ultimately failed to persuade the Supreme Court to hear the case (with no reason given)[37].

[35] Supreme Court of the United States, 'Jane Does No. 1-6, et al., v. Reddit, Inc' (https://supremecourt.gov, 7 March 2023) <https://www.supremecourt.gov/DocketPDF/22/22-695/256427/20230307113426301_22-695ReplyBriefOfPetitioners.pdf> accessed 7 August 2023.

[36] Allow States and Victims to Fight Online Sex Trafficking Act of 2017, Pub. L. No. 115-164 (2018), https://www.govinfo.gov/app/details/PLAW-115publ164.

[37] United States Supreme Court, 'Order List (05/30/2023)' (https://supremecourt.gov, 30 May 2023) <https://www.supremecourt.gov/orders/courtorders/053023zor_d18f.pdf> accessed 17th August 2023.

1.2 Potential to challenge the Proposal before the CJEU

Coming back to the situation in the EU, it is not just academics, politicians, NGOs and advocates who have questioned the legality of the proposal. In her recent paper, Quintel[38] looks at the Opinion published by the Council Legal Service (CLS)[39] which raises significant concerns in relation to the safeguards, e2ee, effectiveness and issues surrounding legal bases for law enforcement processing and criminalising behaviour that is not criminalised in all Member States.

In regards the interference of online communications, there is also a substantial body of case law[40] from the Court of Justice of the European Union - particularly in relation to the indiscriminate collection and retention of communications meta data.

Given that the Proposal would require monitoring of content data (which is generally regarded as requiring stronger protection than meta data,) it seems unlikely that the Proposal would survive a challenge in the Courts - a matter which may well present should Breyer's litigation be referred to the CJEU.

There is also the possibility that, - should the Proposal be adopted, - it could face an annulment in the General Court within two months of the publication of the Regulation in the Official Journal under Article 263(1) of the Treaty on the Functioning of the European Union (TFEU)[41].

Such an action could be initiated by Member States or various EU institutions as 'privileged applicants'. One such Member State that might choose to bring such an action is Austria - which reportedly does not approve of the proposal.[42]

However, an additional avenue would potentially allow even 'non-privileged applicants' by natural or legal persons, to proceed - if they can prove direct individual concern

[38] Dr. Teresa Quintel, 'European Union · Renewed Concerns About Compliance of the Proposed 'Regulation to Prevent and Combat Child Sexual Abuse' with Essence of Right to Data Protection: The Council Legal Service Opinion' (2023) 9 European Data Protection Law Review 173.

[39] Opinion of the Legal Service of the Council of the European Union on the Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, Document No. 8787/23, Brussels, 26 April 2023. The written opinion of the Council Legal Service is not officially available online, but can be requested via the document register under no. 8787/23. A leaked version of the document is available at <https://www.patrick-breyer.de/wp-content/uploads/2023/05/st08787.en23-leak.pdf> access 23 August 2023.

[40] Joined Cases C-793/19 and C-794/19, Joined Cases C-293/12 and C-594/12, Joined Cases C-203/15 and C-698/15 an so forth.

[41] Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union (2016) OJ C 202.

[42] Meineck, Köver and Meister, 'Interne Dokumente zeigen, wie gespalten die EU-Staaten sind' (https://netzpolitik.org, 12 September 2022) <https://netzpolitik.org/2022/chatkontrolle-interne-dokumente-zeigen-wie-gespalten-die-eu-staaten-sind/> accessed 29 August 2023.

cause by the Regulation; and given the broad scope of the Proposal such a claim might well have standing.

Thus it is clear that even prior to considering whether or not the Proposal would meet the requirements of suitability, necessity and proportionality required under Article 5(4) of TFEU; the Proposal faces significant challenges and opposition.

The next section will explore these TFEU issues in more detail whilst looking at the suitability of the Proposal from a technical perspective.

2. Suitability

TFEU Article 5(4) lays down the principle of proportionality which must be met for all EU measures, requiring that such measures must pass three tests. This section will be focused on the first test of 'suitability to achieve the desired end"[43].

Whereas there is no question that the issue of CSAM online is grave and should be addressed - there are questions as to the suitability of the measures proposed.

Although the Proposal is supposed to be technologically neutral (which in itself was subject to criticism in the CLS Opinion as being too vague,) any measure to detect, remove and report such CSAM online will require the use of technology. Given the scale of the problem and the amount of digital communications which take place in the EU every single day.

2.1 Challenges related to the high number of reported material

According to Statistica[44] even a conservative estimate as to the amount of digital communications sent per minute (globally) is around 251.5 million and these numbers only include emails, text messages, Snapchat, Twitter (now X), Instagram and Facebook shares.

If we were to consider all online forum posts in addition to that number, all private messages, video game chats and so on - that number would be significantly higher. Hence although there are currently no clear statistics available to identify the total number of digital communications that occur in the EU every single day, one can safely extrapolate based on the Statistica data.[45]

When including all other forms of digital communications that would be within the scope of the Proposal we are likely to find (conservatively) that in the EU alone, over 100 billion digital communications are sent and received daily.

[43] Glossary of Summaries, 'Principle of proportionality' (https://eur-lex.europa.eu, unknown date) <https://eur-lex.europa.eu/EN/legal-content/glossary/principle-of-proportionality.html> accessed 17 August 2023.

[44] Stacy Jo Dixon, 'Media usage in an internet minute as of April 2022' (https://statistica.com, 6 July 2023) <https://www.statista.com/statistics/195140/new-user-generated-content-uploaded-by-users-per-minute/> accessed 9 August 2023.

[45] Given that the EU contains approximately 1/14 of the global population and based on 251.5 x 60 x 24 (daily number) we see that a conservative estimate puts that number at 362 Billion / 14 = 25 Billion.

According to a report on Swiss news site Republik, in recent years, "the Swiss Federal Police Fedpol recorded a share of up to 80 percent of CSAM reports from the USA that are not relevant under criminal law."[46]

It is important to note that these numbers currently only represent the reporting of known CSAM which is verified by a service provided by the National Centre for Missing and Exploited Children (NCMEC) and only includes material in relation to non-encrypted communications.

The Proposal would require detection of new CSAM across a range of communications services including those which utilise e2ee and as such would result in a significant increase in reporting. Further, the detection of new CSAM is likely to lead to higher error rates as currently reports are vetted by humans but the sheer scale of the reporting required by the Proposal would require the use of automated solutions purely as a matter of practicality.

NCMEC also provides reports to EU law enforcement authorities (LEAs) and Europol in relation to CSAM hosted in the EU and the Irish Council for Civil Liberties (ICCL) shared statistics from An Garda Síochána indicating at least an 11% false positive rate (incorrectly categorising images which were not CSAM as CSAM) with questions remaining as to other terms used, stating that "The true number of false positives is likely to be higher".[47]

To be clear, these are reports are generated through the use of Microsoft's PhotoDNA technology (licensed to NCMEC) and is the technology which is currently favoured by online platforms and SoMe such as Facebook and Twitter.

This seriously calls into question the suitability of the current best in class solutions for the problem of CSAM which the EU Commission is seeking to solve with the Proposal.

[46] Von Eva Wolfangel, 'Die dunklen Schatten der Chatkontrolle' (https://republik.ch, 8 December 2022) <https://www.republik.ch/2022/12/08/die-dunklen-schatten-der-chatkontrolle> accessed 17 July 2023.

[47] Irish Council for Civil Liberties, 'An Garda Síochána unlawfully retains files on innocent people who it has already cleared of producing or sharing of child sex abuse material' (https://iccl.ie, 19 October 2022) <https://www.iccl.ie/news/an-garda-siochana-unlawfully-retains-files-on-innocent-people-who-it-has-already-cleared-of-producing-or-sharing-of-child-sex-abuse-material/> accessed 19th July 2023.

If we put that into context based on a briefing document by the European Parliament[48] there were 32 million reports of 'suspected' CSAM in 2022 by NCMEC based on the perceptual hashing[49] technology, PhotoDNA.

Based on the error rates we have seen from the Swiss and Irish police, this would mean that approximately 25.5 million of those reports would not be criminally actionable and 3.5 million of those reports would not even be CSAM[50].

In addition, one must consider that in 2019, according to the United States Securities and Exchange Commission (SEC), 94% of CSAM reported came directly from Facebook[51] so if we were to apply the Proposal to all 'relevant information society services' in the EU these numbers would be much higher.

Such numbers spell out serious concerns in relation to the people whose communications would be falsely flagged as CSAM and the risks to their fundamental rights and freedoms.

In an attempt to move away from relying on organisations in third countries (such as NCMEC) the Proposal creates a new EU Centre which will (among other responsibilities[52]) 'create, maintain and operate' its own database. This database will rapidly outpace the NCMEC database given the scope and mandatory nature of the Proposal but will face the same issues in relation to accuracy as it will still be populated by data provided through technologies such as PhotoDNA.

One can clearly see that such numbers would be completely overwhelming for EU police forces and the EU Centre which would be setup as a result of the Proposal.

[48] Mar Negreiro, 'Combating child sexual abuse online' (https://europarl.europa.eu, June 2023) <https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/738224/EPRS_BRI(2022)738224_EN.pdf> accessed 19 August 2023.

[49] Perceptual Hashing is based on the content of a digital file and unlike cryptographic hashing can identify images which are the same even if they have been subjected to minor modifications such as resizing.

[50] Based on 80% not being criminally actionable as per the Swiss Fedpol data and the 11% false positive rate as per ICCL, respectively.

[51] United States Securities and Exchange Commission, 'Notice of Exempt Solicitation' (https://sec.gov, 27 May 2020) <https://www.sec.gov/Archives/edgar/data/1326801/000121465920004962/s522201px14a6g.htm> accessed 20 August 2023.

[52] "The EU Centre should also carry out certain complementary tasks, such as assisting competent national authorities in the performance of their tasks under this Regulation and providing support to victims in connection to the providers' obligations. It should also use its central position to facilitate cooperation and the exchange of information and expertise, including for the purposes of evidence-based policy-making and prevention. Prevention is a priority in the Commission's efforts to fight against child sexual abuse." (the Explanatory Memorandum).

2.2 Technological Shortcomings

And this is using the 'state of the art' technological solutions - but as stated, the Proposal does not state which technical solutions should be used and as such it is likely many smaller online platforms will use cheaper and less accurate solutions based on cryptographic hashing algorithms; as whereas the EU Centre has a mandate to provide a database of 'indicators' it is only required to 'facilitate access to reliable detection technologies' rather than provide such technologies or mandate a specific technology.

The current 'best in class' solution (PhotoDNA) uses a methodology known as 'perceptual hashing' which is based on the content of a file as opposed to its structure as a series of bits.

Perceptual hashing is favoured as it can also detect images which are essentially the same but may have been slightly modified (such as the brightness or colouration) making it easier to detect copies of existing CSAM.

Cryptographic hashing detection techniques are easily circumvented. Any change to the file at all (even changing the resolution or simply changing a single pixel) will result in a failed hash check. Despite this cryptographic hashing has been used extensively (even by NCMEC) in the past for the detection of CSAM, it is cheaper, requires fewer technical resources and is faster.

In that vein, a paper[53] by McKeown and Buchanan raises serious concerns even for perceptual hashing technologies like PhotoDNA. Their paper compares 1 million public images against control images to determine how well perceptual hashing algorithms handle detection attacks and discovered that even the simple mirroring of an image (flipping it on the X axis) or placing a border around the image can be enough to confuse these perceptual hashing algorithms (including PhotoDNA).

Further, as the NCMEC database grows it becomes increasingly susceptible to 'hash collisions' known in cryptography as the Birthday Problem (or Pigeonhole Principle).

This principle dictates that if you have a finite number of containers but a higher number of items to go in the containers - at least some of the containers will have more than one item.[54]

[53] McKeown and Buchanan, 'Hamming Distributions of Popular Perceptual Hashing Techniques' (2022) DFRWS (Digital Forensics Research Conference) EU 2023, 21-24 March 2023, Bonn, Germany.

[54] Arthur Bellore, 'Birthday Attacks, Collisions, And Password Strength' (https://auth0.com, 23 March 2021) <https://auth0.com/blog/birthday-attacks-collisions-and-password-strength/> accessed 27 August 2023.

This means that as any hash database grows, the chances of two different images creating the same hash grows, leading to further false positive and false negative situations because it could be that an image which is not CSAM will generate the same hash value as an existing CSAM image leading to a false positive - or that a new CSAM image will create a hash that is the same as a non-CSAM image resulting in a false negative.

Given that reporting of CSAM (which involves the sending of the images to NCMEC in most circumstances) is currently voluntary, the NCMEC database is relatively small and, in 2019 it contained only 69.1 million hashes according to the SEC report mentioned above.

However, it is likely that, should the Proposal become law, based on the sheer number of digital communications which would be monitored, we are likely to see both the NCMEC database grow exponentially (as 'relevant information society services' will still forward reports to NCMEC as well as the EU Centre) and the EU Centre which the Proposal would create[55] would face the same accuracy issues - seriously limiting the suitability of the Proposal.

[55] Chapter IV of the Proposal.

2.3 Risks arising from the emergence of Generative Artificial Intelligence

Furthermore, we need to consider the rapid emergence of Generative Artificial Intelligence (GenAI) with regards to the generation of synthetic media. Thiel, Stroebel and Portnoff[56] address the legal concerns relating to synthetic CSAM created by generative AI models such as as 'Diffusion'.

Their article discusses a number of mitigations to prevent the abuse of GenAI to create CSAM such as specifically training models to be biased against the creation of child nudity and, watermarking[57].

The problem is these mitigations can be circumvented through techniques such as adversarial attacks as described by Kos, Fischer and Song in their paper[58] among others.

This means that, in essence, any safeguards which are deployed through the training of AI to prevent generation of harmful content (such as CSAM) can be attacked with adversarial models to circumvent those safeguards creating a cycle of mitigation and circumvention.[59]

Hence, for the time being it seems unlikely that there will be a suitable mitigation against GenAI creating CSAM and as we can already see, GenAI is increasingly being used to generate synthetic CSAM as recently reported by The Washington Post[60].

GenAI is able to create synthetic CSAM in only a few seconds, making it an effective tool for the gratification of those who consume CSAM and according to NGO Out of The Shadows in a recent index report "Over 40% of countries assessed for the index either do not explicitly define 'child pornography' or 'child sexual abuse material' in national legislation, or their definitions do not meet international standards"[61].

[56] Thiel, Stroebel and Portnoff, 'Generative ML and CSAM: Implications and Mitigations' (https://stacks.stanford.edu, 24 June 2023) <https://stacks.stanford.edu/file/druid:jv206yg3793/20230624-sio-cg-csam-report.pdf> accessed 17 August 2023.

[57] Watermarking is a method for identifying data similar to how a bank note might have a watermark. Such marks (in theory) cannot be removed and thus can serve as a source for authenticating the data or determining its origin.

[58] Kos, Fischer and Song, 'Adversarial examples for generative models' (https://arxiv.org, 22 February 2017) <https://arxiv.org/pdf/1702.06832.pdf> accessed 12 August 2023.

[59] As one solution is found to overcome one adversarial attack another attack is created specifically to break the previous solution.

[60] Drew Harwell, 'AI-generated child sex images spawn new nightmare for the web' (https://washingtonpost.com, 19 June 2023) <https://www.washingtonpost.com/technology/2023/06/19/artificial-intelligence-child-sex-abuse-images/> accessed 21 June 2023.

[61] Out of the Shadows, 'Index 2022' (https://cdn.outoftheshadows.global, 8 Feb 2023) <https://cdn.outoftheshadows.global/uploads/documents/OOS_Index_Global_Report_2022_EN_V2_2023-

Some even argue that synthetic CSAM should be legal as it might work as an alternative source of material that does not involve the physical or sexual abuse of a real person thus gratifying those who consume it in a way which does not cause harm as posited by Ole Martin Moen and Aksel Braanen Sterri in their paper[62].

Given the low cost and ease of access to GenAI generators it is clear that GenAI will have a significant impact on the CSAM debate. One the one hand as a result of the Internet being flooded with synthetic CSAM thus making it far more difficult to find real CSAM. On the other hand, as a means to convert real CSAM into synthetic CSAM (such as 'cartoonification') in order to avoid detection by technologies such as PhotoDNA.

2.4 Policy considerations on synthetic CSAM and deep fakes

Additional issues will emerge as Legislators attempt to deal with the issue of synthetic CSAM. For instance, should synthetic CSAM be considered as a harmless solution providing an outlet for sexual gratification to pedophiles or should it be considered as a gateway to child sexual abuse?

Further concerns arise around the weaponising of synthetic CSAM against public figures such as journalists, politicians, human rights campaigners and celebrities.

In April 2018[63], investigative journalist and writer Rana Ayyub was targeted after speaking on television news (BBC and Al Jazeera) on the issue of child sexual abuse in India. The next day her Twitter account was hacked to send highly charged messages such as "I hate India and Indians!" and "I love Pakistan" and then later was informed of a pornographic video being circulated on WhatsApp. The video was synthetic pornography otherwise known as a 'deepfake' depicting Ayyub engaged in various sexual acts which never actually happened.

The video was being shared by over and over by members of the nationalist Bharatiya Janata Party (BJP) who had been marching in support of a BJP member and law

02-08-174957_kmfz.pdf> accessed 28 August 2023.

[62] Ole Martin Moen and Aksel Braanen Sterri, 'Pedophilia and Computer-Generated Child Pornography' (https://olemartinmoen.com, 2018) <https://www.olemartinmoen.com/wp-content/uploads/Pedophilia-and-computer-generated-child-pornography.pdf> accessed 17 June 2023.

[63] Rana Ayyub, 'I was the victim of a deepfake porn plot intended to silence me' (https://huffingtonpost.co.uk, 21 November 2018) <https://www.huffingtonpost.co.uk/entry/deepfake-porn_uk_5bf2c126e4b0f32bd58ba316> accessed 19th August 2023.

maker accused of raping an 8 year old Kashmiri girl[64] - the very story that Ayyub had spoken about in her televised interviews.

As Ayyub states "From the day the video was published, I have not been the same person. I used to be very opinionated, now I'm much more cautious about what I post online. I've self-censored quite a bit out of necessity."

This is one of the first known cases of deepfakes or synthetic pornography being used to chill free speech. Respected US civil rights lawyer, Danielle Keats Citron, writes about Ayyub and other similar cases in her book[65] and warns that the future will be littered with similar stories.

The use of GenAI to weaponise CSAM will be instrumentalised by nation states to embarrass their critics or meet other political agendas. It will be used by politicians to weaken their opponents, will be used by individuals for personal gain, revenge and other purposes and will be used by companies for profit.[66]

As the rise of GenAI continues the creation of synthetic CSAM will become easier and this author predicts that within the next 3 years there will likely be major campaigns involving synthetic CSAM used to attack politicians and journalists, political dissidents and celebrities - exacerbating the issue and overwhelming law enforcement.

It is also likely that such cased will be the focus of law enforcement given the significant public interest such attacks will create - this will lead to fewer resources to investigate real CSAM, putting children at risk rather than helping to protect them.

Arguably, the EU Commission's proposal will contribute to this problem due to the potentially incredible increase in the number of reports sent by SoMe and other platforms and the high false positive and false negative rates being reported.

[64] Krishna N. Das and Rupam Jain, 'BJP MLA arrested over rape as protests mount' (https://reuters.com, 13 April 2018) <https://www.reuters.com/article/india-rape-bjp-cbi-idINKBN1HK0NT> accessed 20 August 2023.

[65] Danielle Keats Citrone, *The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age* (1st edn, W. W. Norton & Company 2022).

[66] There are currently hundreds of celebrity deepfake pornography sites on the Internet in what Arwa Mahdawi at The Guardian states "is an emergency that is ruining lives." Mahdawi cites a 2019 report by Sensity (no longer publicly available) stating that most synthetic pornography is non-consensual (96%) and overwhelmingly targets women (99%).

3. Problems related to criminalising behaviour, lack of evidence based data and risk of circumvention

3.1 Criminalising consensual sexual conduct

Another issue which policy makers face is that of teenagers engaged in 'sexting'[67]. Police in Germany published information in April 2023[68] stating that 42% of investigations into online CSAM were targeted at minors (under 18) engaging in 'sexting'.

This would indicate that the Proposal, should it become law, would lead to the investigation and in many cases, prosecution of vast numbers of teens simply exercising their natural curiosity and sexuality. This would not be a constructive use of the law and would again divert attention and investigative resources away from actual pedophiles, causing genuine harm.

In essence such an approach would have the opposite impact the EU Commission had intended with their Proposal in that it would both fail to protect children from sexual predators (due to the issues outlined above) whilst at the same time criminalising our youth in their pursuit of their sexual identity.

3.2 Problems of evidence-based numbers put forward in the Proposal

In May 2022 the EU Commission issued a press release announcing the Proposal stating that "The COVID-19 pandemic has exacerbated the issue, with the Internet Watch foundation noting a 64% increase in reports of confirmed child sexual abuse in 2021 compared to the previous year."[69]

As such one further needs to question the EU Commission's reasoning given the evidence they have presented states that the amount of CSAM is increasing.

Given that some online services have been detecting and reporting CSAM for years (using technologies such as PhotoDNA) and even the Derogation making such activities

[67] Sexting is the consensual creation and dissemination of sexually explicit material via communications services and is common among teenagers and young adults.

[68] Polizeiliche Kriminalprävention der Länder und des Bundes, 'Verbreitung von Kinderpornografie nimmt 2022 weiter zu' (https://polizei-beratung.de, 19 April 2023) <https://www.polizei-beratung.de/aktuelles/detailansicht/straftat-verbreitung-kinderpornografie-pks-2022/> accessed 17 June 2023.

[69] European Commission, 'Fighting child sexual abuse: Commission proposes new rules to protect children' (https://ec.europa.eu, 11 May 2022) <https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2976> accessed 2 August 2023.

lawful has not seen any decrease (to the contrary, the anecdotal numbers the EU Commission provide suggest the problem is getting worse) and as such it is likely that the Proposal will not see any significant decrease either.

Had the Derogation led to a reduction in CSAM rates it might be arguable that such a policy is effective but the reality is that actually, things are going in the opposite direction or at least, that is how it seems. However, given there has been no formal assessment of the Derogation it is difficult to ascertain what the actual rates are and one should question why the EU Commission has not conducted such an assessment or released any further data on efficacy of the Derogation.

For example, a Meta press release in February 2021, the company stated that "more than 90% of the reported content was the same as or visually similar to previously reported content. In addition, copies of just six videos were responsible for more than half of the child exploitative content we reported in that time period."[70]

In the same press release, Meta states that in more than 75% of cases they researched dissemination of the CSAM 'did not exhibit malicious intent', again raising questions as to the real numbers of actionable and unique CSAM reports.

Thus, it could be argued that the EU Commission might be misleading legislators in the Parliament and Council by including reports related to identical or very similar images in their lobbying for support of the Proposal as none of the explanatory memorandums, press releases or commissioned reports seem to mention these issues.

Hence, on the one hand we see the numbers of unique images reduced by 90%[71] leading to significant over reporting. On the other hand we see 75% of reported behaviour was (albeit inexcusable) simply irresponsible rather than malicious, failing to establish *mens rea*[72] required in many jurisdictions to secure a criminal conviction.

This is not to say that the numbers of genuine CSAM images are not still a concern because just as the false positive rate could lead to massive amounts of people being wrongly accused. The relatively low percentage of malicious CSAM still represents large numbers - albeit much lower than being presented by the EU Commission. Evidently, any number of victims is too many

[70] Antigone Davis, 'Preventing Child Exploitation on Our Apps' (https://about.fb.com, 23 February 2021) <https://about.fb.com/news/2021/02/preventing-child-exploitation-on-our-apps/> accessed 19 August 2023.

[71] Based on Meta's research above.

[72] Mens rea is the legal concept of state of mind (intent) required along with actus reus (the criminal act) to successfully prosecute a crime.

However, the subsequent section will consider the Proposal's suitability form the perspective of circumvention.

3.4 Challenges related to the dark web

The Onion Router (TOR) otherwise known as 'the dark web' has long been known to be a haven for sexual predators due to the anonymous nature of the network.[73]

TOR sits on top of the traditional Internet and uses a large network of decentralised servers to act as proxies that encrypt the data and shield the user from discovery. It cannot be access via the usual methods of typing in a easily remembered web site address such as google.com or facebook.com.

Instead, TOR addresses are created cryptographically and can only be accessed once a user is connected to a TOR entry node (or gateway) usually through a special TOR capable web browser that also serves to initiate the connection to the entry node.

In a second step, just like in a Hollywood spy movie, the user's browser requests are sent from one proxy server to another, to another until it reaches an 'exit node' at which point it connects to the requested dark web resource (such as a web site or chatroom).

The servers between the entry node and the exit node neither receive information about the browser requests nor the identity or Internet address of the user - as all of that data is encrypted. The purpose of these so-called circuit nodes are purely to route the information anonymously between the entry and exit nodes.

As such, TOR is a popular haven for illegal markets selling drugs, identities, stolen credit cards, prostitution, weapons and sex trafficking and other criminal activities.

In a short paper, Roberta Liggett O'Malley states that '80% of hidden service traffic is dedicated to web sites hosting CSAM[74]. Therefore, a large portion of commercial CSAM is conducted through anonymous web software."

For that reason, TOR has long been a thorn in the side of law enforcement as it works incredibly well at anonymising criminal activities[75]. However, despite multiple efforts to

[73] Andy Greenberg, 'Over 80 Percent of Dark-Web Visits Relate to Pedophilia, Study Finds' (https://wired.com, 30 December 2014) <https://www.wired.com/2014/12/80-percent-dark-web-visits-relate-pedophilia-study-finds/> accessed 25 July 2023.

[74] Roberta Liggett O'Malley, 'Commercial Child Sexual Abuse Markets on the Dark Web' (https://cj.msu.edu, June 2018) <https://cj.msu.edu/_assets/pdfs/cina/CINA-White_Papers-Liggett_Commercial_Child_Sexual_Abuse_Markets_Dark_Web.pdf> accessed 27th July 2023.

[75] Dave Lee, 'Defending Tor - gateway to the dark web' (https://bbc.com, 5 August 2017) <https://www.bbc.com/news/technology-40810771> accessed 17 July 2023.

take control, success stories are rare and as soon as one site is taken down - just like the proverbial hydra, a new one replaces it - usually with identical content (known as a 'mirror'). It is unlikely that this issue will be resolved outside of outlawing TOR.

Due to the distributed nature of the TOR network, no single Country can effectively shut it down as the TOR network nodes will simply move to a new jurisdiction. Because the network encrypts all routing and content data it is impossible to even detect a TOR connection as it looks no different to traffic for Internet banking, shopping on Amazon or reading the news on the BBC. This is the designed purpose of Tor (and web encryption generally) - to protect the content of the communications from interception and interference.

Just as a significant amount of TOR traffic is reportedly used for CSAM purposes *O'Malley (fn 74)*, if the Proposal becomes law, the easiest way for CSAM consumers and distributors to remain undetected is to simply move to TOR.

However, even if those consumers would not trust TOR there would be many other options available should one wish to cover their tracks, as will be explained in the following sections.

3.5 Understanding communications networks

If we are to assess the suitability of the Proposal from the perspective of circumvention techniques, it is critical to understand how the underlying technologies of modern communications networks work.

The Internet consists of millions of machines (servers) located all across the globe and accessed via special names (domain names managed through the domain name system (DNS)) such as google.com or bbc.com.

These names are translated by special servers known as 'nameservers' into a special number known as an IP address. These IP addresses need to be publicly addressable to be accessible over the Internet. By this, they must be in specific IP addresses ranges (classes) which have been designated and publicly available.

Yet, there is another type of IP address which is not publicly addressable and therefore cannot be accessed directly via the Internet. These special classes of IP addresses are reserved for private networks such as the ones run by corporations in their offices or even the network of devices one might have at home.

For example - most of us have a home internet connection which has a single publicly addressable IP address - this allows us to receive information from remote servers such as those used by web sites and mobile applications. Without a publicly addressable IP address these servers would not be able to send back the information or web pages that we request through our apps and web browsers.

However, every device in our home usually shares the same public IP address through what is known as Network Address Translation (NAT). This NAT system allows for information sent to our public IP address to be delivered to the specific device that requested it. It ensures that the data requested does not go to the wrong device by mapping the request to a private IP address (which is not publicly addressable).

These private IP addresses (for example 192.168.1.24) can only be seen and accessed by other devices in the same address space. Hence, in the above example, only machines which have an IP address in the range of 192.168.1.0-255 can access the machine with the IP address 192.168.1.24 and in order for other devices in different networks to be able to access that same machine - they need to be able to use a "bridge" which connects the two networks together. This is essentially what NAT does - it provides that bridge so that different networks can communicate with each other (other types of network bridges exist but are not relevant for the purpose of this example).

Everything which happens on a private network is hidden from the public Internet (and TOR is basically just one giant - albeit quite sophisticated, private network where the entry and exit nodes can be considered as the bridges). This means if a file is sent from one device to another over a private home network - it is not detectable by anyone outside of that network including law enforcement.

This is useful for network security as it enables us to secure our local network activities and files from external parties but it also enables us to hide our unlawful activities as well.

3.6 The use of VPNs and additional private networks and similar

Just as TOR works through a set of distributed private network nodes a similar distributed network of private network nodes may be set up in a number of different ways.

A Virtual Private Network (VPN) is one such method. Essentially, a VPN is used to encrypt traffic and access resources on a device that does not have a publicly addressable IP address (it is behind a NAT router). In this case, the VPN becomes the bridge which connects a local device to the device or resource on the remote private network.

All communications between the respective user's device and the resources on the private network are encrypted, which is why VPNs are often used by organisations to provide remote access to their network. This is particularly useful for remote workers as this method provides secure access to company resources.

However, just as a company can setup a VPN, this may be done any individual person. No particular hardware required and the software that creates these bridges is free and open source in many cases[76].

An indefinite number of people can access the hidden resources through the VPN, the sole requirement is that they are in possession of the access credentials. Once connected to the VPN, any type of data can be exchanged, including CSAM, and be completely undetectable to anyone not connected to the VPN.

VPNs and TOR are not the only types of networks that are useful for hiding unlawful activities. Mesh networks work in a similar way to VPNs in that they bridge multiple private networks together in a 'mesh'.

Mesh networks have existed almost as long as computer networks have but have seen something of a resurgence in recent years as a means to combat issues over net neutrality .

[76] Paul Bischoff, '6 open source tools for making your own VPN' (https://opensource.com, 31 August 2018) <https://opensource.com/article/18/8/open-source-tools-vpn> accessed 30 August 2023.

For instance, where internet service providers slow down or speed up certain access to resources usually based on monetisation of content[77].

One feature of mesh networks is the ability to disseminate masses of data automatically via peer-to-peer sharing. In such cases no single individual holds all the data. Instead it is distributed among the mesh nodes in order to ensure that the data is still available to everyone else via the other nodes should one node go offline[78].

The technologies used for Mesh networks are very similar to storage technologies known as a Redundant Array of Inexpensive Disks (RAID)[79] a storage technique designed to prevent data loss - where parity data (data that describes the stored data in such a way as it can be recovered if it is damaged) stored across all devices connected to the Mesh network, is used to rebuild the blocks of data that were hosted on the disconnected node.

Similar to the above examples, these networks are encrypted and invisible to the public Internet and consequently law enforcement. However, an additional advantage of such systems is that often no individual holds a full copy of the data. Instead, each individual user holds just pieces and when another user opens a file on a mesh network, the network will automatically download the missing pieces or recreate blocks using parity techniques *PhoenixNAP (fn 79)*.

As such, any pedophile who may be concerned at being discovered, can simply delete any complete data on their devices and recover it at any time from other nodes in the network when they feel secure enough to do so. This also allows pedophiles to travel across borders with their devices without the fear of having evidence discovered in the case of a search.

There are many more examples of other types of private networks. Even older techniques such as steganography (a method of hiding data within other data[80]) would be enough to thwart current detection methods. Fayyad-Kazan, Saba, Hejase et al. explore these issues in their paper and discuss real criminal cases including that of the pedophile

[77] Mark Kaufman, 'Mesh networks: An alternative way to connect to the internet gains steam' (https://mashable.com, 9 January 2018) <https://mashable.com/article/mesh-networks-provide-alternative-intenet-connection> accessed 12 May 2023.

[78] Resilio, 'The Benefits of Using Peer-to-Peer Mesh Network Technology to Overcome Connectivity Issues' (https://resilio.com, date unknown) <https://www.resilio.com/usecases/overcoming-poor-connectivity/> accessed 30 August 2023.

[79] PhoenixNAP, 'What is RAID?' (https://phoenixnap.com, 23 July 2019) <https://phoenixnap.com/kb/raid-levels-and-types> accessed 30 August 2023.

[80] Kaspersky, 'What is steganography? Definition and explanation' (https://kaspersky.com, unknown date) <https://www.kaspersky.com/resource-center/definitions/what-is-steganography> accessed 28 August 2023.

ring known as “Shadowz Brotherhood”.[81] Therefore this thesis argues that the Proposal would not help to manage the issue of pedophiles, who could simply move their activities to such networks or countries that are out of reach of EU enforcement.

[81] Fayyad-Kazan, Saba, Hejase et al., ‘JPEG Steganography: Hiding in Plain Sight’ (2021) 6(1) International Journal of Forensic Sciences <https://medwinpublishers.com/IJFSC/jpeg-steganography-hiding-in-plain-sight.pdf> accessed 12 August 2023.

4. Conclusion

Further issues arise given that the scope of the EU Commission Proposal is limited to 'relevant information society services'[82]. This means that as soon as it becomes law, pedophiles using e2ee encrypted commercial services are likely to move to other non-commercial services or use open source technologies (as discussed above) to create their own private networks.

Even a ban of e2ee in relation to existing commercial services such as Facebook Messenger, Telegram or WhatsApp will not prevent pedophiles from using encryption, steganography and other techniques that are all based on open source and freely available technologies. As famous cryptologist Phil Zimmermann puts it "You can't ban math"[83].

Given all of the above information and the requirements of Article 5(4) of the TFEU on suitability, necessity and proportionality - it is difficult to see how the Proposal even passes the first test of achieving the desired end given that:

1. The current state of the art technological solutions are do not achieve the necessary accuracy rates, creating a large number of false positives and are likely to become even less accurate over time due to the above-mentioned 'Birthday problem' and emergence of synthetic CSAM;
2. Detection is trivial to circumvent by using a range of free solutions such as private networks and obfuscation techniques including steganography and encryption;
3. The Proposal's scope is restricted to commercial platforms leading to the inevitable use of non-commercial platforms which are not obligated to actively detect CSAM;
4. Enforcement issues in regions outside of the EU.

Additional issues such as a lack of consistency in relation to the age of consent not just globally but within the EU itself, consensual CSAM created by and distributed by minors in the exploration of their own sexuality, and the lack of resources for law enforcement in the face of an extreme and rapid increase in reports[84] add to the problems.

[82] See Article 2 - Definitions

[83] Phil Zimmermann, "'Crack Down' on Crypto? Maybe, but You Can't Ban Math" (https://uk.news.yahoo.com, 3 March 2022) <https://uk.news.yahoo.com/crack-down-crypto-maybe-t-211241142.html> accessed 19 July 2023.

[84] Tweede Kamer, 'Europese Verordening ter voorkoming en bestrijding van seksueel kindermisbruik' (Dutch) (https://debatgemist.tweedekamer.nl, 4 October 2022) <https://debatgemist.tweedekamer.nl/node/29579> accessed 29 August 2023.

Even if the Proposal will be adopted there is no guarantee that the law will not be annulled by the CJEU.

Therefore, this thesis argues that alternative solutions need to be considered as the online world is becoming increasingly sexualised but arguably not because of pedophiles. The hyper-sexualisation of teenagers and young adults (made to look like teenagers) in our society (both online and offline) is increasing.

For example, the advertising industry has been long criticised for the sexualisation of minors[85] but the same issues exist across popular media, entertainment and other industries such as fashion.

This is not a new trend. However, the Internet and SoMe in particular, have contributed to the countless hypersexualised 'influencers' on Instagram, Tik Tok and other modern media platforms. Even now, five years since the '#MeToo' campaign started, we continue to see reports of inappropriate sexualisation of minors across these sectors and more recently also in sports[86].

If as a society we permit celebrities to commit sexual assault without consequence; allow giant corporations to profit from the hypersexualisation of minors; allow popular media such as the movie and music industry to hypersexualise child actors and musicians; and the fashion and advertising industries to profit from sexualisation of minors - how then can we argue that this is wrong?

Such hypocrisy only serves to normalise such behaviour, encourage it and worse, lead young girls to believe that the only way they can succeed in life is to show flesh and make themselves sexually available.

Thus, before we start to turn teenagers engaged in sexting, into criminals for exploring their own sexuality - it might be more prudent to focus our efforts on these issues of sexualisation and hypersexualisation of minors as discussed above, that normalises such behaviour.

Instead of invading the private spheres of our lives for the purpose of detecting CSAM which in many cases might not actually be CSAM and is not actionable - the focus

[85] Camillia Dass, 'Italian fashion brand Benetton next under fire for sexualising children in new ad' (https://marketing-interactive.com, 5 January 2023) <https://www.marketing-interactive.com/italian-fashion-brand-benetton-is-under-fire-for-sexualising-children-in-a-new-ad> accessed 30 August 2023.

[86] Molly McElwee, 'Special investigation: The whistleblowers driving Sport's #MeToo movement' (https://www.telegraph.co.uk, 27 May 2021) <https://www.telegraph.co.uk/womens-sport/2021/05/27/sexual-harrassment-athletics-abuse-sports-metoo/> accessed 29 August 2023.

should be set on education and awareness raising, studying the reasons why pedophiles exhibit such behaviour and supporting the victims and survivors of abuse.

One thing is clear - the EU Commission themselves have already admitted in their own press release that this solution does not work - despite the derogation making such activities lawful since 2021 and platforms using PhotoDNA for many years before that - we have seen no decrease in these crimes, to the contrary - we only see an increase.

As such, by their own admission, the EU Commission has to accept that their Proposal is not suitable to meet its stated goals and as such fails the first test of Article 5(4) of the TFEU thus requiring no further consideration of the other two tests for necessity and proportionality.

Personal Testimony

There is no question that this thesis has focused on the failings of the Proposal and that is because there is a great deal to be said when it comes to efficacy and proportionality issues. But that doesn't mean that the Commission's intent is bad or that the entire proposal is bad.

As someone who has studied these issues for decades (this author's last major academic dissertation was titled "Issues of Paedophilia on the Internet" and was an analysis largely focused on §230 of CDA back in 1997) one must acknowledge that at least there is recognition that a policy strategy is required to address this issue (however misplaced that current strategy might seem).

The creation of an EU Centre is clearly needed to lead such a strategy, create policy, provide resources (financial and educational) and mediate between different stakeholders (including victims and survivors who have been woefully under-represented during these policy debates).

If one thing alone can be salvaged from the Proposal, it should be the EU Centre because any strategy requires a foundation and such a Centre could serve well as that foundation to build stronger, more effective policy in the future, whilst leading research not just into mitigation but actual prevention.

And this is perhaps where the Proposal fails the most - it fails the victims and the survivors by focusing too much on mitigation (preventing the dissemination of CSAM online) whilst failing to address the Mastodon in the room - that once the CSAM material reaches the Internet, the abuse has already occurred.

By focusing purely on the use of online platforms to disseminate CSAM the Proposal misses a key opportunity to study why pedophiles exhibit such behaviour in the first place. For it is only our understanding of the cause which will eventually lead to a strategy of prevention. Simply focusing on the CSAM material whilst failing to address causation will never achieve the goal of preventing children from being subjected to rape and other forms of sexual assault.

As it stands we still see little to no meaningful support for victims and survivors (particularly survivors of abuse from many years back who have since come forward and reported the crimes against them) particularly in relation to financial support for the trauma such abuse manifests and the impact that has on the life of those abused.

As someone with first hand experience of reporting sexual and physical abuse leading to multiple convictions - this author has never been offered any support either therapeutic, financial or any other form of support. To the contrary, this author was simply forgotten about once convictions were secured - no follow up from law enforcement, no reach out from social services or mental health professionals and no acknowledgement or compensation for the impact such abuse has had one one's life.

This needs to change, this is why this thesis is so personal and so important to this author because we cannot continue to hide painful truths behind inadequate technology and public policy simply because it is too difficult to discuss in a more appropriate and effective way.

Aside from the many issues discussed in this thesis - the one thing not yet discussed is the impact such a policy would have on the very people the Commission claims to want to protect - victims and survivors.

We need our safe spaces, we need the freedom to conduct confidential communications, we need our remaining fundamental rights to privacy and data protection to allow us to live our lives in a way which respects our human dignity.

Without confidential communications it is likely that the issue of non-reporting will remain, as the simple act of telling our stories is incredibly difficult due to a lack of trust, personal shame and embarrassment, worry of being stigmatised and even questions relating to our own sexuality.

As a survivor of child sexual abuse this author is all too familiar with these feelings and concerns which is why it took 20 years for this author to report the crimes against them; and whereas that reporting eventually led to multiple convictions it was only the availability of encrypted messaging and secure communications which gave this author the courage to tell their story.

Victims and survivors have already suffered so much violence and attacks on their human dignity, their hearts, their bodies and their minds. It is not appropriate to subject them to further violence by attacking their privacy.

We are broken and we try every day to put ourselves back together but policy proposals such as the Commission's do nothing to address that and serve only to delegate responsibility to a magic black box that is accountable to no-one and is trusted with blind faith.

Hopefully, this thesis has highlighted some of the significant issues the Proposal creates and has illustrated that without meeting the requirements of suitability such a Regulation would not be lawful under the TFEU.

Perhaps in some small way, this thesis will encourage politicians and legislators to look at addressing the cause of such heinous behaviour and divert EU funds towards more research on these issues, rather than using those same EU funds to buy silicon bandaids which will do nothing to stop the wounds festering and merely cover up that which needs to be exposed.

I finish with the words of my old psychology professor who was my mentor and support 26 years ago as I struggled with my own abuse when writing my previous dissertation on these matters. His words remain with me and motivate my work and I will forever be thankful for the strength he gave me to follow this difficult avenue of research.

If one finds a child drowning in a canal the obvious answer is to jump into the canal and save the child - it is a noble and honourable thing to do. Yet, if one travels further down the canal and finds more children drowning than they can possibly save - surely it makes more sense to head upstream and discover why the children are ending up in the canal in the first place.

We will never overcome the issue of child sexual abuse - it is an issue as old as civilisation and sadly there will always be people in this world who have a sexual preference for children. However, if we study the cause, if we try to understand why this preference exists, perhaps we can at least reduce it - this will not happen simply by focusing on the CSAM disseminated after the fact.

It is time for the Commission to reconsider their approach for the sake of democracy, for the sake of fundamental rights, for legal certainty and for the lives of those children and survivors they claim they are trying to protect.

They cannot continue to waste time and resources on ineffective and arguably unlawful policies; they must respect EU case law and treaties if they are to provide the legal certainty required for policy to be effective.

There are no easy answers to these issues and there is no magic bullet available from technology because this is a human problem that requires human intervention.

There is only one thing more difficult than trying to find a needle in a stack of hay and that is trying to find the same needle in an even larger stack of identical needles.

*

One hopes this thesis has illustrated just how large that stack of needles is likely to become as a result of the surveillance of hundreds of billions of communications per day; and how emerging technologies create additional threats which are likely to divert resources away from real abuse in order to deal with weaponised synthetic CSAM.

The future for this issue is deeply troubling, we need to look for and find real solutions.

Bibliography

1. European Commission Proposal 2020/0259 (COD). Available at https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2020/0568/COM_COM(2020)0568_EN.pdf (Accessed on 14th June 2022)

2. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L201/37

3. Microsoft Inc., 'PhotoDNA' (https://www.microsoft.com, date unknown) <https://www.microsoft.com/en-us/photodna> accessed 12 August 2023

4. Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast)Text with EEA relevance. [2018] OJ L321/36

5. European Commission Proposal 2022/0155 (COD). Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN&qid=1652451192472 (Accessed on 14th June 2022)

6. Dr. Teresa Quintel, 'The Commission Proposal on Combatting Child Sexual Abuse - Confidentiality of Communications at Risk?' (2022), European Data Protection Law Review 262

7. European Digital Rights Initiative, 'Private and secure communications attacked by European Commission's latest proposal' (https://edri.org, 11 May 2023) <https://edri.org/our-work/private-and-secure-communications-put-at-risk-by-european-commissions-latest-proposal/> accessed 9 August 2023

8. Patrick Breyer MEP, 'Chat Control: The EU's CSEM scanner proposal' (https://patrick-breyer.de, date unknown) <https://www.patrick-breyer.de/en/posts/chat-

control/> accessed 17 August 2023

9. German Bundestag Research Services, '"Chat control" - Analysis of the EU Commission's draft regulation 2022/0155 (COD)(English translation)' (https://patrick-breyer.de, 7 October 2022) <https://www.patrick-breyer.de/wp-content/uploads/2022/10/221007-WD-10-026-22-Bewertende-Analyse-zur-Chatkontrolle_EN-1.pdf> accessed 7 August 2023

10. Charter of Fundamental Rights of the European Union [2012] OJ C326/391

11. Steinmeier, '20220509_Unterlassungsklage_Facebook_Breyer' (https://patrick-breyer.de, 9 May 2022) <https://www.patrick-breyer.de/wp-content/uploads/2022/05/20220509_Unterlassungsklage_Facebook_Breyer.pdf> accessed 17 July 2023

12. Patrick Breyer MEP, '"Destruction of digital privacy of correspondence": lawsuit filed against chat control' (https://patrick-breyer.de, 10 May 2022) <https://www.patrick-breyer.de/en/destruction-of-digital-privacy-of-correspondence-lawsuit-filed-against-chat-control/> accessed 29 July 2023

13. Prof. Dr. Ninon Colneric, 'Legal opinion commissioned by MEP Patrick Breyer, The Greens/EFA Group in the European Parliament' (https://patrick-breyer.de, March 2021) <https://www.patrick-breyer.de/wp-content/uploads/2021/03/Legal-Opinion-Screening-for-child-pornography-2021-03-04.pdf> accessed 13 March 2023

14. YouGov, 'Omnibus International - Topic: Chat Control - 10 countries' (https://nextcloud.pp-eu.eu, April 2021) <https://nextcloud.pp-eu.eu/index.php/s/5bkdRGyxnAciNBz?dir=undefined&openfile=372951> accessed 14 March 2023

15. European Data Protection Board and European Data Protection Supervisor, 'Joint Opinion 4/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse'

(https://edps.europa.ee, 28 July 2022) <https://edps.europa.eu/system/files/2022-07/22-07-28_edpb-edps-joint-opinion-csam_en.pdf> accessed 17 June 2023

16. Cornell Law School, '47 U.S. Code § 230 - Protection for private blocking and screening of offensive material' (https://law.cornell.edu, date unknown) <https://www.law.cornell.edu/uscode/text/47/230> accessed 20 August 2023

17. Apple Inc., 'Expanded Protections for Children' (https://apple.com, 5 August 2021) <https://www.apple.com/child-safety/> accessed 22 August 2023

18. Information Privacy Commissioner of Ontario, 'Privacy by Design' (https://ipc.on.ca, January 2018) <https://www.ipc.on.ca/wp-content/uploads/2018/01/pbd-1.pdf> accessed 3 February 2023

19. Author unattributed, 'An Open Letter Against Apple's Privacy-Invasive Content Scanning Technology' (https://appleprivacyletter.com, 6 August 2021) <https://appleprivacyletter.com/> accessed 22 August 2023

20. Cornell Law School, '47 U.S. Code § 230 - Protection for private blocking and screening of offensive material' (https://law.cornell.edu, date unknown) <https://www.law.cornell.edu/uscode/text/47/230> accessed 20 August 2023

21. Supreme Court of the United States, 'Search Results' (https://supremecourt.gov, 30 May 2023) <https://www.supremecourt.gov/search.aspx?filename=/docket/docketfiles/html/public/22-695.html> accessed 7 July 2023

22. Allow States and Victims to Fight Online Sex Trafficking Act of 2017, Pub. L. No. 115-164 (2018), https://www.govinfo.gov/app/details/PLAW-115publ164

23. Dr. Teresa Quintel, 'European Union · Renewed Concerns About Compliance of the Proposed 'Regulation to Prevent and Combat Child Sexual Abuse' with Essence of Right to Data Protection: The Council Legal Service Opinion' (2023) 9 Eu-

ropean Data Protection Law Review 173

24. Joined Cases C-793/19 and C-794/19 *Bundesrepublik Deutschland v SpaceNet AG (C-793/19), Telekom Deutschland GmbH (C-794/19)* [2022]

25. Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and Others (C-594/12)* [2014]

26. Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post- och telestyrelsen (C-203/15), Secretary of State for the Home Department v Tom Watson, Peter Brice, Geoffrey Lewis (C-698/15)* [2016]

27. Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union (2016) OJ C 202

28. Glossary of Summaries, 'Principle of proportionality' (https://eur-lex.europa.eu, unknown date) <https://eur-lex.europa.eu/EN/legal-content/glossary/principle-of-proportionality.html> accessed 17 August 2023

29. Stacy Jo Dixon, 'Media usage in an internet minute as of April 2022' (https://statistica.com, 6 July 2023) <https://www.statista.com/statistics/195140/new-user-generated-content-uploaded-by-users-per-minute/> accessed 9 August 2023

30. Von Eva Wolfangel, 'Die dunklen Schatten der Chatkontrolle' (https://republik.ch, 8 December 2022) <https://www.republik.ch/2022/12/08/die-dunklen-schatten-der-chatkontrolle> accessed 17 July 2023

31. Irish Council for Civil Liberties, 'An Garda Síochána unlawfully retains files on innocent people who it has already cleared of producing or sharing of child sex abuse material' (https://iccl.ie, 19 October 2022) <https://www.iccl.ie/news/an-garda-

siochana-unlawfully-retains-files-on-innocent-people-who-it-has-already-cleared-of-producing-or-sharing-of-child-sex-abuse-material/> accessed 19th July 2023

32. Mar Negreiro, 'Combating child sexual abuse online' (https://europarl.europa.eu, June 2023) < https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/738224/EPRS_BRI(2022)738224_EN.pdf> accessed 19 August 2023

33. United States Securities and Exchange Commission, 'Notice of Exempt Solicitation' (https://sec.gov, 27 May 2020) <https://www.sec.gov/Archives/edgar/data/1326801/000121465920004962/s522201px14a6g.htm> accessed 20 August 2023

34. McKeown and Buchanan, 'Hamming Distributions of Popular Perceptual Hashing Techniques' (2022) DFRWS (Digital Forensics Research Conference) EU 2023, 21-24 March 2023, Bonn, Germany

35. Arthur Bellore, 'Birthday Attacks, Collisions, And Password Strength' (https://auth0.com, 23 March 2021) <https://auth0.com/blog/birthday-attacks-collisions-and-password-strength/> accessed 27 August 2023

36. Thiel, Stroebel and Portnoff, 'Generative ML and CSAM: Implications and Mitigations' (https://stacks.stanford.edu, 24 June 2023) <https://stacks.stanford.edu/file/druid:jv206yg3793/20230624-sio-cg-csam-report.pdf> accessed 17 August 2023

37. Kos, Fischer and Song, 'Adversarial examples for generative models' (https://arxiv.org, 22 February 2017) <https://arxiv.org/pdf/1702.06832.pdf> accessed 12 August 2023

38. Drew Harwell, 'AI-generated child sex images spawn new nightmare for the web' (https://washingtonpost.com, 19 June 2023) <https://www.washingtonpost.com/technology/2023/06/19/artificial-intelligence-child-

sex-abuse-images/> accessed 21 June 202

39. Ole Martin Moen and Aksel Braanen Sterri, 'Pedophilia and Computer-Generated Child Pornography' (https://olemartinmoen.com, 2018) <https://www.olemartinmoen.com/wp-content/uploads/Pedophilia-and-computer-generated-child-pornography.pdf> accessed 17 June 2023

40. Rana Ayyub, 'I was the victim of a deepfake porn plot intended to silence me' (https://huffingtonpost.co.uk, 21 November 2018) <https://www.huffingtonpost.co.uk/entry/deepfake-porn_uk_5bf2c126e4b0f32bd58ba316> accessed 19th August 202

41. Danielle Keats Citrone, *The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age* (1st edn, W. W. Norton & Company 2022)

42. Arwa Mahdawi, 'Nonconsensual deepfake porn is an emergency that is ruining lives' (https://theguardian.com, 1 April 2023) <https://www.theguardian.com/commentisfree/2023/apr/01/ai-deepfake-porn-fake-images> accessed 2 August 2023

43. Polizeiliche Kriminalprävention der Länder und des Bundes, 'Verbreitung von Kinderpornografie nimmt 2022 weiter zu' (https://polizei-beratung.de, 19 April 2023) <https://www.polizei-beratung.de/aktuelles/detailansicht/straftat-verbreitung-kinderpornografie-pks-2022/> accessed 17 June 2023

44. European Commission, 'Fighting child sexual abuse: Commission proposes new rules to protect children' (https://ec.europa.eu, 11 May 2022) <https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2976> accessed 2 August 2023

45. Antigone Davis, 'Preventing Child Exploitation on Our Apps' (https://about.fb.com, 23 February 2021) <https://about.fb.com/news/2021/02/preventing-child-exploitation-on-our-apps/> ac-

cessed 19 August 2023

46. Thomas Van der Valk, ‘Effectively sfaeguarding children against online abuse.’ (https://youtube.com, 22 June 2023) <https://youtu.be/5DLQE7AGHaA?feature=shared&t=1025> accessed 19 August 2023

47. Roberta Liggett O’Malley, ‘Commercial Child Sexual Abuse Markets on the Dark Web’ (https://cj.msu.edu, June 2018) <https://cj.msu.edu/_assets/pdfs/cina/CINA-White_Papers-Liggett_Commercial_Child_Sexual_Abuse_Markets_Dark_Web.pdf> accessed 27th July 2023

48. Mark Kaufman, ‘Mesh networks: An alternative way to connect to the internet gains steam’ (https://mashable.com, 9 January 2018) <https://mashable.com/article/mesh-networks-provide-alternative-intenet-connection> accessed 12 May 2023

49. Kaspersky, ‘What is steganography? Definition and explanation’ (https://kaspersky.com, unknown date) <https://www.kaspersky.com/resource-center/definitions/what-is-steganography> accessed 28 August 2023

50. Fayyad-Kazan, Saba, Hejase et al., ‘JPEG Steganography: Hiding in Plain Sight’ (2021) 6(1) International Journal of Forensic Sciences <https://medwinpublishers.com/IJFSC/jpeg-steganography-hiding-in-plain-sight.pdf> accessed 12 August 2023

51. Phil Zimmermann, “‘Crack Down’ on Crypto? Maybe, but You Can’t Ban Math” (https://uk.news.yahoo.com, 3 March 2022) <https://uk.news.yahoo.com/crack-down-crypto-maybe-t-211241142.html> accessed 19 July 2023

52. Neil Sears, ‘Police 'not interested' in Wyman's affair with 13-year-old Mandy Smith, who claims she slept with him when she was 14’ (https://dailymail.co.uk, 1 April 2013) <https://www.dailymail.co.uk/news/article-

2301867/Bill-Wyman-Police-interested-Rolling-Stones-affair-13-year-old-Mandy-Smith-claims-slept-14.html> accessed 3 July 2023

53. Rebecca Sayce, 'Brooke Shields still struggling to understand why her mother let her pose naked aged 10 and play prostitute aged 11' (https://metro.co.uk, 27 march 2023) <https://metro.co.uk/2023/03/27/brooke-shields-asks-why-mother-let-her-star-in-nude-scenes-aged-11-18506942/> accessed on 19 August 2023

54. Lauren Tuck, 'Is 8-Year-Old Kristina Pimenova the Most Beautiful Girl in the World?' (https://yahoo.com, 5 December 2014) <https://www.yahoo.com/lifestyle/is-8-year-old-kristina-pimenova-the-most-beautiful-104422161308.html> accessed 12 August 2023