SEPTEMBER 2022

Protecting Children from Sexual Abuse

Thorn's View on the EU Commission's Pioneering Proposal

THORN

INTRODUCTION

We are Thorn – a nonprofit organization that builds technology and programs to defend children from sexual abuse. We aim to share our experience and technical expertise with all relevant stakeholders, especially those at the forefront of protecting children online.

The EU Commission's proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse ("the Proposal') is a groundbreaking piece of legislation. It has the potential to not only protect the ongoing work in this space, but to enhance the entire ecosystem in effectively tackling child sexual abuse online. This Proposal is a critical step toward better protection of children worldwide and further enshrines safety principles.

The dissemination of child sexual abuse material (CSAM) online has dramatically increased in recent years and continues to rise. Many digital stakeholders already engage in **significant voluntary mitigation efforts** – however, the lack of legal certainty presents a key hurdle to progress in the global fight against the dissemination of CSAM across the internet and has led to harmful detection gaps. We must ensure effective legislation is in place so that children are free to explore and learn safely online.

At Thorn, we know that collective action is the only way to stop the spread of CSAM online. It takes collaboration between citizens, institutions, policymakers, tech companies, and nonprofit organizations alike.

We also know that many tech companies are already taking important steps to counter the rise of CSAM on their platforms. The proposal will further drive companies in the right direction by prioritizing prevention and **safety by design.** By entrusting tech companies to conduct risk assessments, the regulation will provide **greater transparency** on the actions undertaken to combat the dissemination of CSAM online and will foster meaningful action. The Proposal will also improve **legal certainty** for companies by clarifying their obligations to detect CSAM.

By proposing detection mandates and the establishment of an EU Centre, the Commission's regulation represents a significant policy shift for the EU. What follows are Thorn's views and recommendations on these two major policy changes.

While we welcome the introduction of detection mandates, Chapter I stresses the importance of tech companies' voluntary efforts to detect CSAM. We call upon EU decision-makers to explicitly **recognise proactive voluntary detection efforts** as essential risk mitigation measures.

Chapter II discusses the capacity of the EU Centre to act as a continental research hub. It will require appropriate **financial, technical, and physical resources** paired with strong privacy and security safeguards and close cooperation between the EU Centre and the existing child protection ecosystem.

At Thorn, we consider the detection of CSAM online as an irreplaceable part of the global fight to protect children. Yet, it constitutes only one part of what is needed. We welcome all the necessary provisions of the Proposal aimed at ensuring the removal of CSAM and fostering victim support. When we work together and implement the measures proposed by the European Commission, we can change the future of the internet and make it safer for children, now and for generations to come.

I

The Case for Safe and Proportionate Proactive Detection

At Thorn, we welcome and value all efforts made to better protect children in online spaces. As instances of online CSAM continue to increase at an alarming rate, the digital ecosystem is meeting the moment in a coordinated effort to cease the dissemination online.

Targeted detection is one of the most powerful tools we can utilise to protect children at scale. These detection measures include all technology built to identify the existence and/or dissemination of known or new CSAM or the solicitation of children, including hashing and matching, classifiers, and anti-grooming tools.

By introducing detection mandates, the Commission recognises detection tools' crucial contribution to tackling and eliminating CSAM online. The Commission also aims to enhance transparency about detection tools by asking providers to inform their users that they are operating detection technologies to fight CSAM and explaining how these technologies function (Art. 10, 5a). We value this recognition and commitment to transparency and call on European lawmakers to make the most of these technologies to empower digital platforms in the fight to protect children online.

Whilst recognising the potential of detection tools, the current version of the Proposal does not allow providers to voluntarily or proactively detect and report CSAM. Under the proposed rules, online service providers would have to wait for a detection order to be able to use such tools. The Commission rightly points out that voluntary action alone will not solve the growing issue of CSAM, which is why we welcome the introduction of detection mandates.

Not all online service providers are willing to deploy detection measures. **It is crucial, however, that proactive detection remains an option for providers who are willing and able to mitigate the spread of CSAM, without a prior detection order.** We believe that any provider should be able to ensure that their platform is free of CSAM, as a safer internet is not only expected by users but also necessary in order for survivors of child sexual abuse to exit the vicious circle of re-victimisation. If maintained, this provision will lead to the disruption of existing processes amounting to significant negative repercussions on the world's fight against CSAM online. **Voluntary and mandatory detection are complementary** and, with the right design, can both be subject to the same legal safeguards.

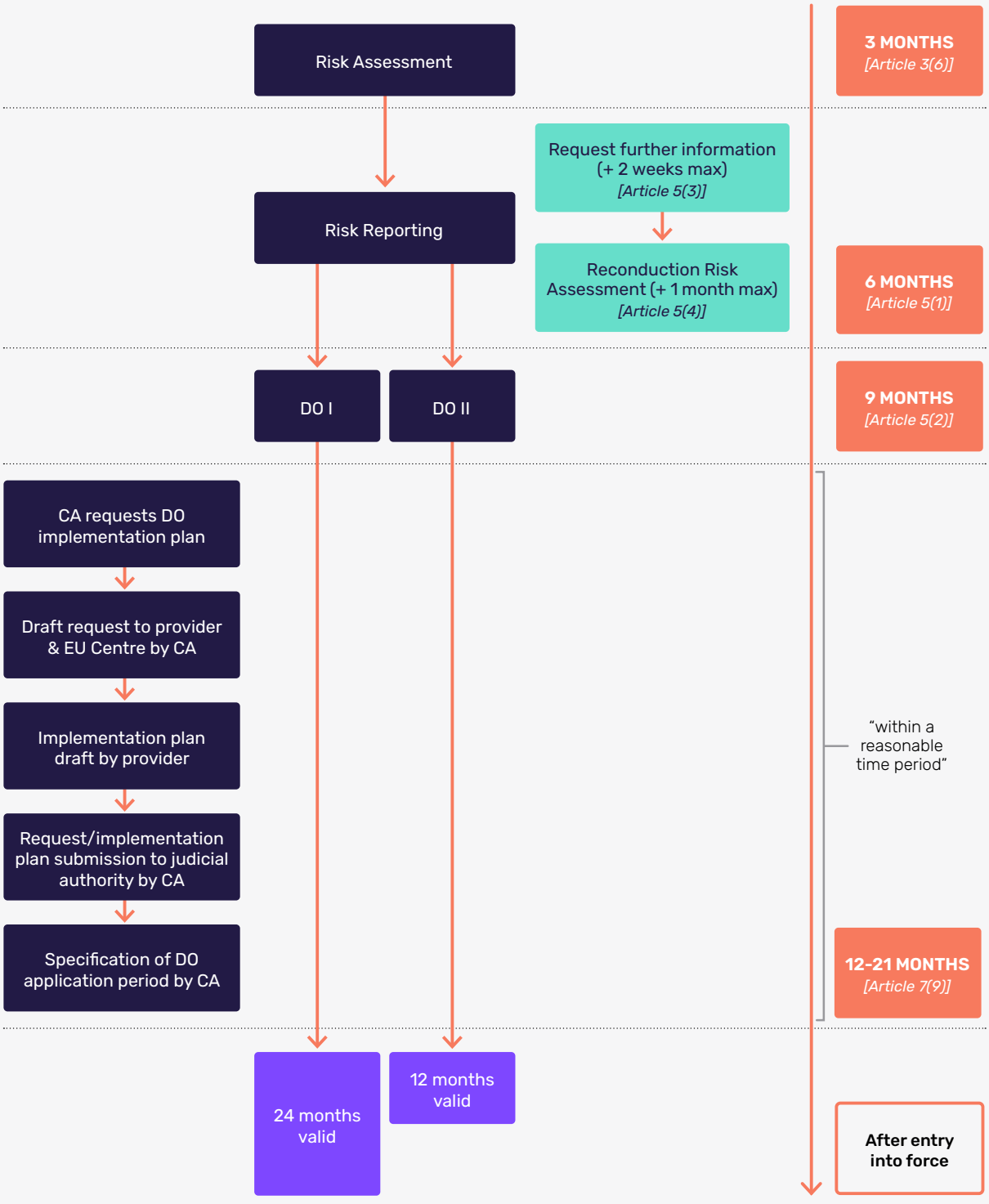
STREAMLINING BUREAUCRACY

The Proposal represents a significant policy shift. It replaces a system that relies solely on providers' voluntary efforts to detect, report and remove CSAM with one geared towards detection mandates for single providers. In fact, providers would only be allowed to deploy detection technologies if they are mandated to do so. Certain providers would be issued "detection orders" through a long bureaucratic and cumbersome process. **Graph 1** illustrates the process that providers would have to go through until a detection order can be issued.

The fundamental issue at the heart of the detection order process is the potential **bottleneck** it risks creating in the absence of a possibility for providers to take proactive voluntary detection measures.

This process could create a delay of one to two years between the entry into force of the legislation and the issuance of the first detections orders. This estimation does not include the time between the request for a plan of a detection order and until the plan is accepted by a judicial authority, which is not specified but will most certainly take several additional months.

GRAPH 1 | Detection Orders (DO)



Start of assessment 3 months after the regulation date of application or 3 months after provider offers service in EU [Article 3(6)]

Update of assessment least once every 3 years or when necessary and at least 2 months before period expire of DO application [Article 3(6)]

DO I = concerning the dissemination of known or new CSAM [Article 7(9)]

DO II = concerning solicitation of children [Article 7(9)]

CA = competent authority

THE RE-EMERGENCE OF HARMFUL DETECTION GAPS

One immediate consequence of the detection orders system proposed by the Commission is the emergence of **harmful detection gaps.**

In the past, legal loopholes in the EU showed the negative impact of detection gaps on child safety: When providers stopped detecting and reporting CSAM in the EU for most of 2021 due to legal uncertainty surrounding the EU's ePrivacy directive, the number of reports of CSAM, according to NCMEC[1], decreased by 58%. The system outlined in the Proposal will lead to even longer detection gaps, as it neglects to include a bridging solution that guarantees the continuous detection by providers between the expiry of the interim derogation and the entering into force of the new legislation. Providers that are currently detecting on a voluntary basis will be forced to stop and wait for years until a detection order is issued. In the meantime, CSAM will undoubtedly circulate freely across the web and law enforcement will lack information essential to their investigations.

UNDERMINING PROVIDER RISK ASSESSMENTS

In the Proposal, the issuance of a detection order will only function as a measure of last resort. The preceding steps consist of conducting a risk assessment and, based on the outcome of the assessment, deploying voluntary risk mitigation measures.

The current version of the Proposal does not allow for voluntary detection – or the highly targeted use of specific detection technology to identify CSAM. This exclusion represents a choice that will undoubtedly and significantly undermine the intended purpose of such an order.

The reality is that while many companies are unaware that their platforms are being misused for the dissemination of CSAM, others are aware but neglect to take action. Without being allowed to use the necessary detection technologies, **providers will not be able to thoroughly assess CSAM-related risks** on their platforms and will remain in the dark about the scale of this crime, even if they know that CSAM is likely present. The Commission's risk assessment approach would, therefore, be flawed.

This constitutes a blind spot in the entire detection order architecture, which is designed to enable the detection of CSAM risks but impedes providers from using CSAM detection tools. It is essential that providers have adequate tools and information at their disposal when conducting their risk assessment.

Our experience in the digital child safety space tells us that far more is needed to make an impact than the three risk assessment measures (age verification, user flagging, and outsourcing the assessment to the EU Centre) suggested in the Proposal.

While age verification is an important preventive tool, especially to protect children from grooming, it does not solely eliminate the spread of CSAM. User flagging and reporting should be a built-in and simplified feature of every service. But this practice has obvious limits, as the processes are not always easy to follow or are overly burdensome.

The third option, outsourcing the assessment to the EU Centre at the provider's own cost, entitles providers to ask the EU Centre to analyse a "representative data set" for CSAM risks. This raises the concern of how and by whom such a sample data set would be chosen. Providers should not be able to evade their responsibilities by picking and sharing data to their liking.

CURTAILING THE USE OF EFFECTIVE MITIGATION MEASURES

Once a provider has conducted its risk assessments, it is asked to **mitigate these risks without the use of detection technologies**. As a result, providers are deprived of the tools to effectively fight a crime they strongly suspect exists on their platforms. Providers should instead deploy "appropriate technical and operational measures

1 CyberTipline Data (missingkids.org)

and staffing" (Art. 4), which can entail measures such as age verification and adapting algorithmic recommender systems – both of which are clearly insufficient when cases of CSAM have already been confirmed. The provision on **appropriate measures is vague, in particular as to which technologies fall into the realm of mitigation measures and which would require a detection order.** This creates legal uncertainty for providers, meaning that they will be hesitant to use and invent new technologies without prior approval by the EU Centre.

STIFLING INNOVATION

Over the past decade, providers' voluntary detection efforts have been crucial for advancing innovation in the world's fight against CSAM online. **The ability to innovate and improve detection technologies has emerged as the backbone of this fight.** Thorn therefore welcomes that the Commission has chosen to follow an overall innovation-friendly approach in its Proposal.

Ruling out proactive detection, however, will unintentionally neutralise one of the main drivers for innovation in this space. Providers know their platforms and what solutions could address these problems. Where no solutions exist, they have to be invented and numerous providers have proven to be extremely effective in doing so. By limiting the space for proactive efforts and prescribing which technologies can be used in detection orders, the Proposal gives providers **little incentive to come up with new solutions or improve existing ones.** What is needed is a solution that better encourages decentralised and proactive innovation by providers.

Thorn's Key Recommendations

Thorn recommends that the Proposal **includes voluntary proactive use of detection technologies that providers can deploy as part of their risk assessment and voluntary risk mitigation efforts.** We contend that a shift in the system is necessary, moving from one relying entirely on mandatory detection orders that are based on incomplete evidence to one that allows providers to voluntarily detect for CSAM on their platforms.

Those providers who are willing to voluntarily detect CSAM as part of their risk assessment or mitigation measures should be able to notify relevant authorities about their activities, the technology they are using, and the results they yield. Those providers who do notify appropriate authorities would follow the same process as those who go through the regular detection process, and would therefore also be subject to the same legal safeguards as well. In the meantime, those providers would have the ability to fight CSAM.

Should the review by authorities reveal that a provider's technology and process do not meet the EU Centre's standards – or that their use of detection technology is unjustified in light of the risks that the provider has identified – authorities could edit or remedy the provider's measures.

This recommendation would prevent the detection order process from becoming a bottleneck while maintaining the checks and balances which ensure that detection technologies are used in a targeted manner and fulfill the highest standards.

Chapter I Recommendations

ARTICLE 3 — RISK ASSESSMENT

- Providers should be able to proactively use detection technologies as part of their risk assessment.
- Providers willing to voluntarily detect CSAM as part of their risk assessment should notify the relevant authorities accordingly.
- Additional safeguards must be put in place to verify that the data which providers forward to the EU Centre for analysis is representative and does not serve the purpose of evading their responsibilities.

ARTICLE 4 — RISK MITIGATION

- The proactive use of detection technologies should be included among the measures providers can deploy to mitigate the risk of CSAM.
- Providers willing to proactively detect CSAM as part of their risk mitigation measures should notify the relevant authorities accordingly.

ARTICLE 7 — ISSUANCE OF DETECTION ORDERS

- Allow for the certification of providers' proactive detection activities in the detection order process.

II

Establishing an Effective EU Centre

Thorn supports the proposed establishment of an **EU Centre, which will serve as a vital pillar of the world's fight against CSAM.** Similar centres already exist in various jurisdictions and have demonstrated their efficiency in centralising detected materials, liaising with enforcement authorities, and providing necessary assistance and support to victims.

With the formation of the EU Centre, the EU has the unique opportunity to tailor its response to the many new and upcoming challenges of this crime and thereby set a global standard for decades to come. Centralising and safeguarding the creation and maintenance of CSAM indicators in an independent European agency marks a big step forward. This centralisation will be critical to avoid creating data silos, which would make it more difficult to protect children.

As a developer of technology, Thorn welcomes the capacity of the EU Centre to act as a regional research hub, and we look forward to potential collaboration in this space. Bearing such paramount yet sensitive responsibilities will **require appropriate financial, technical, and physical resources paired with strong privacy and security safeguards.** The EU Centre must therefore retain a high degree of independence from political and law enforcement institutions and have its own financial as well as human resources. In order to strengthen the global fight to eradicate CSAM, cooperation between the EU Centre and the existing child protection ecosystem needs also to be laid out in more detail.

Finally, the EU Centre and its Technology Committee will play a vital role in reviewing new technologies. Critical to this mission is the ability of the EU Centre **to provide robust and timely advice to ensure that technologies are effective,** allowing for fast paced innovation needed to tackle an ever-evolving crime.

INDEPENDENCE OF THE EU CENTRE

Close cooperation between the EU Centre and Europol is essential for an effective fight against CSAM. The EU Centre will act as a go-between for private providers and law enforcement: it will receive and assess reports from providers and, if a report is found to contain CSAM, will forward it to Europol. Exercising this intermediary role **independently** will contribute to the efficiency of the process and citizens' trust in the EU's fight against CSAM online. It will ensure that reports to law enforcement are accurate and that the relevant intelligence is shared fast and seamlessly with the right authorities. The sensitivity of the EU Centre's work warrants that its everyday operations are completely separate from law enforcement agencies.

In its current draft, the Commission's Proposal does not achieve this objective. Notably, according to article 53 of the proposed regulation, the EU Centre will share and thus depend on Europol's human resources management, staff, IT systems, and other administrative functions. While this may produce some cost efficiencies, there is a risk that such joint functions may compromise the EU's Centre's independence.

Thorn's Recommendation

Thorn recommends that the **EU Centre's status as an independent EU agency is reflected in its finance and structure.** To this end, it should run its own budget, human resources management, staff, and security system. This does not preclude the mutual representation of Europol and EU Centre officials on the management boards, provided that such officials are able to act independently.

INTEGRATING THE EU CENTRE IN THE GLOBAL ECOSYSTEM

The global fight against CSAM is a carefully orchestrated effort. In order to strengthen proven procedures, the EU Centre must fit neatly into the global ecosystem. Cooperation with existing and future regional centres of reporting is crucial yet not detailed in the Proposal. Reporting centres must be able to work with each other to safely share information and reports when necessary. They often receive this information first, and quick action is vital to ensure children at risk are found. Therefore, we would welcome further details about how different centres can cooperate whilst safeguarding privacy and personal data.

ADOPTING, DISSEMINATING, AND MAINTAINING NEW DETECTION TECHNOLOGY

By acting as a central research and innovation hub, the EU Centre has the potential to act as a catalyst of change in the fight against CSAM. In that respect, it is very important that the Centre has the necessary capabilities, financing, and tools to assume this responsibility. Given the fast-paced technological environment in which perpetrators operate, it is crucial that the Centre can act equally fast. **To this end, smooth and efficient procedures to adopt, disseminate, maintain, and improve detection technologies are vital for the EU Centre.**

The Technology Committee in the EU Centre will play a particularly important role in these processes and therefore holds a great deal of responsibility for the entire technical and civil society ecosystem. We welcome its creation and feel it will provide important trust between technology and wider society. The Technology Committee's ability to give opinions on existing and new detection technologies creates a new level of transparency and will incentivise innovation in this area.

Thorn's Recommendations

Given this crucial role, the legislation should **further clarify the composition and governance of the Technology Committee.** In order to properly validate technology, the Committee will need to be composed of technical experts who are able to act independently of service providers, as well as law enforcement experts who can assess whether detection technology is proportionate to the scale and severity of the crime. In addition, we propose that the Technology Committee have civil society representation to ensure a balanced view on the impact of CSAM-related crime as well as the tools used to fight this crime on individuals, society and privacy.

DATA RETENTION AND ACCESS TO DATA

In order for law enforcement to be able to tackle child sexual abuse and protect children effectively, access to data is a key component. The EU Centre will verify the reports for law enforcement, but law enforcement officials often need additional data from a service provider. Article 22 of the Proposal specifies that data cannot be held for longer than 12 months but it fails to establish a minimum retention period.

Without a minimum retention period, companies could report to the EU Centre and immediately delete the information. In a space where every image is a crime scene, every piece of evidence is vital. We encourage the insertion of a finite minimum retention period for companies in regards to any data related to an EU Centre report. Access to the database of indicators is also a precondition for providers and organisations to detect CSAM and improve their detection tools. Article 46 ties providers' access to these indicators to the execution of detection orders.

As Thorn advocates for allowing proactive detection under this regulation, **providers should not be barred from accessing these databases if they decide to detect voluntarily.** Article 46 also limits access to these databases to providers and law enforcement agencies, thereby excluding the many organisations that are vested in the fight against CSAM, be it through building detection technology or providing detection services. The importance of including diverse stakeholders in the fight against CSAM is set forth in Article 54, which lends the EU Centre the competence to conclude memoranda of understanding with partner organisations. These memoranda of understanding open the door for various possibilities for cooperation, among which requesting access to the Centre's databases should be included. Limiting such access to providers only would fall short of leveraging the diversity of relevant stakeholders.

Thorn's Recommendation

To prevent providers from immediately deleting material related to EU Centre reports, Thorn **suggests a minimum retention period of at least 6 months for relevant material.** This period would grant law enforcement agencies sufficient time to assess data that may be relevant for their investigations.

Finally, we recommend that **partner organisations with whom the EU Centre concludes memoranda of understanding have the option to request access to the wide array of databases** the EU Centre will establish if this pertains to the EU Centre's task. This option should be enshrined in Article 46.

Chapter II Recommendations

ARTICLE 22 – PRESERVATION OF INFORMATION

- Providers shall preserve material related to EU Centre reports for at least 6 months from the date of the reporting or of the removal or disabling of access, whichever occurs first.

ARTICLE 40 – ESTABLISHMENT AND SCOPE OF ACTION OF THE EU CENTRE; ARTICLE 67 – BUDGET ESTABLISHMENT AND IMPLEMENTATION; ARTICLE 69 – BUDGET

- The EU Centre's status as an independent EU agency should be reflected in its finance and structure.
- It should run its own budget, human resources management, staff and security system and not rely on other bodies for support in these areas.

ARTICLE 46 – ACCESS, ACCURACY AND SECURITY

- Providers should be able to request access to the EU Centre's database for the purpose of their proactive detection efforts.
- Partner organisations which concluded memoranda of understanding with the EU Centre should have the option to request access to the databases of indicators if this pertains to the EU Centre's task.

ARTICLE 54 – COOPERATION WITH PARTNER ORGANISATIONS

- There should be further details about how different centres can cooperate whilst safeguarding privacy and personal data.
- Draw out more clearly how civil society organisations can engage with the EU Centre and continue to provide their unique added value.

ARTICLE 66 – ESTABLISHMENT AND TASKS OF THE TECHNOLOGY COMMITTEE

- More clarification is needed about the composition and governance of the Technology Committee.
- In order to properly validate technology, the Committee should comprise of technical experts who are able to act independently of service providers, as well as law enforcement experts who can assess whether detection technology is proportionate to the scale and severity of the crime.
- The Technology Committee should have civil society representation to ensure a balanced view on the impact of CSAM-related crime as well as the tools used to fight this crime on individuals, society and privacy.

III

Encryption

Thorn believes that we can simultaneously ensure privacy and protect children. To build a world where every child can safely use the internet, we must design safety into our technology, including encrypted spaces. We do not support governments inserting backdoors. **We support encrypted spaces that are privacy-forward, in which companies can detect for both known and unknown CSAM images and videos.**

Encrypted environments are invaluable technological tools that protect user privacy and allow for the safe transfer of data and information. Encryption comes in many forms – from what is used to secure our bank accounts, to encrypted tunnels for emails, to full end-to-end encrypted environments. **At Thorn, we know that strong encryption is a necessity and believe that there are balanced approaches which can allow for the detection of CSAM in encrypted environments.**

The Proposal does not specifically name encryption or any technologies as it is aimed at being tech-neutral in order to evolve with the changing technological landscape. We applaud this effort as we at Thorn know how quickly technology can evolve. This legislation is very clear that a detection order cannot be issued unless technology exists to detect in that environment. This is an important safeguard to ensure that secure spaces remain secure and any technology used for the detection of CSAM is used solely for this purpose.

As we work to find solutions to keep all online spaces safer for children, it's critical that we encourage creativity, willingness to detect, and the ability to develop a multitude of potential solutions. As a result, those with an interest in protecting children have options from which to derive the most effective ones. An environment where ongoing innovation is encouraged is the only way to solve this nuanced problem. As technology evolves, safety by design must be ingrained into a company's business plans. Striving to create privacy-forward, safe environments should be a fundamental principle as technology progresses. This legislation strives to balance what currently exists and creates a safer online world.

Now is the time to have these conversations. Encryption is a vital part of technology and we can find a balance that ensures privacy whilst not allowing for children to be exploited and CSAM to be spread unchecked on public platforms. Tackling CSAM at scale requires a holistic approach – this includes looking at all types of technology and all solutions.

FOR MORE INFORMATION PLEASE CONTACT:

[redacted]