HACKATHON CHILD FOCUS & NTT

April 25 to 26, 2024

Child Focus

NTT DATA

Thank you for dedicating your valuable time and expertise to contribute to our society, particularly for the benefit of our children. To aid you in choosing a challenge, Child Focus has created concise and intriguing briefs for each option. Step into the perspective of each persona to gain insight into the challenges and aspirations faced by Child Focus. We hope this serves as a useful starting point as you embark on your journey.

"If I had an hour to solve a problem I'd spend 55 minutes thinking about the problem and 5 minutes thinking about solutions."

— **Albert Einstein**

Child Focus

Child Focus is the Belgian Foundation for Missing and Sexually Exploited Children. Established in 1998, in the aftermath of the widely known “affaire Dutroux”, characterized by the brutal abductions and sexual abuse of Julie, Mélissa, An, Eefje, Leatitia, and Sabine. Over the years Child Focus became the leading Belgian Safer Internet Centre in collaboration with Mediawijs, Média Animation and Conseil Supérieur de l’éducation aux Médias.

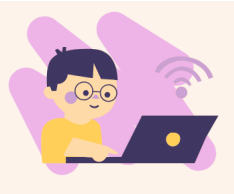
Safeguarding children and youth from contemporary threats and violence, particularly in the online realm, is a critical and pressing concern in our modern society. While the exponential growth of the Internet has brought numerous benefits, it has simultaneously exposed children to new risks and threats.

Staying abreast of the rapid advancements in technology poses a considerable challenge, especially for children, who often find it difficult to navigate this evolving landscape. This is evident in the significant increase in cases reported to our services. Currently, child protection services grapple with limited resources and extensive waiting lists.

How can we ensure the safety of our children? We require technology-driven solutions that address both current challenges and emerging needs. To achieve this, we seek your assistance! Contribute your skills and time to our emergency call. Five challenges await your engagement, each playing a vital role in guaranteeing the paramount safety of our children.

The 5 challenges

During the hackathon, the different teams will be invited to tackle 5 crucial challenges for the organization:



Easy way for children to report their online nightmares to Child Focus

Stop the spread of abusive images across platforms

Well-being of analysts confronted with violent content

Balancing between different rights: Privacy and Protection

Working with technology to identify and manage information on new threats

Challenge 1

Child inviting and friendly reporting portal: how can Child Focus make it easier for minors to report their online nightmares?

Child Focus aims to develop accessible, secure and child-friendly tools to lower barriers for minors to report. These tools will need to ensure complete confidentiality.

“I have your nudes” (1/2)

In recent years, helplines worldwide witnessed a sharp increase in reports of online sexual exploitation of children. Children, more than ever, use the endless opportunities of the internet to shape their identities, including their sexual selves. Engaging in online sexual experimentation is not in itself problematic; however, it is not without risk. Children are being lured, coerced, misled, or their trust breached into producing and sharing intimate pictures of themselves. Once their nudes are out there, their whole world collapses. Feelings of shame, panic, loneliness and shock can be so overwhelming that, in extreme circumstances, it has ended in suicide in a short time span of 4 hours following the initial contact.

This is what happened to Glenn... Appelez Glenn (French) Bel Glenn (Dutch)

How can we make sure they get help in time so we can save them from their online nightmares?

Main hurdles

- Our communication channels (24/7 emergency line, peer-to-peer platforms, online form for reporting child sexual abuse images) do not effectively reach children directly.
- Children are facing many barriers to reporting: fear of victim blaming, fear of their parent's reactions, cultural barriers, and police consequences,...
- Content takedown is not guaranteed and relies on the willingness of platforms.
- Legal restriction: Child Focus is prohibited from having and maintaining a database of content.

Help us achieve our ambition

Contribute to the development of an easy and accessible Belgian portal for children and youngsters at risk of having their intimate images spread.

Challenge 2

Sharing intimate and abusive images of children is not caring: How can we effectively raise awareness and educate the public to stop sharing such images?

Child sexual exploitation pictures (e.g. self-generated material) circulate extensively across the internet and various platforms. These images become viral often due to a lack of understanding on how to appropriately respond to such content.

“I have your nudes” (2/2)

We refer to the above story of thousands of youngsters like Glenn, who are confronted with the horrible reality that they have been exposed to, and their private photos may be circulating online on platforms such as Instagram, Snapchat, Telegram, or other social media. In many cases, we observe individuals sharing these images or participating in exposure groups, often unaware that online actions can have a tremendous impact on the real-life experiences of their peers. While this is a distressing fact, our commitment is to fight against this phenomenon and work towards creating a safer online environment... Appelez Glenn (French) Bel Glenn (Dutch)

What can bystanders or witnesses do?

Main hurdles

- Change of mindset: encourage the public to take immediate action.
- Public awareness: following a media intervention, we typically see a peak at our hotline, but it fades away quickly. How can we maintain visibility?
- Overcoming reporting barriers: It requires people to fill in several fields, fear of the follow-up and consequences...

Help us achieve our ambition

Encourage all bystanders to report indecent images instead of sharing them.

Challenge 3

How can we facilitate decompression in a high-level stress environment?

Child Focus analysts are exposed to violent and extreme content (e.g. Child Sexual Abuse Material) on a daily basis, impacting their well-being. Child Focus is seeking for technology-based safeguarding solutions to reduce image exposure and to preserve their wellbeing.

“Behind the scenes, behind the screens”

“You are never fully prepared for what may come.”

Every two days, I enter the secure environment in Child Focus, not knowing what I will see that day. With a single click, I find myself locked with the eyes of a child. Experiencing horrendous pain and suffering. I try to limit my gaze. Within seconds I scan the image and determine: Is this a child? Is this child victim of child sexual abuse? Two questions, two answers. I swipe the image down within seconds to limit my exposure and move swiftly to another screen, where I trace and report the image to the competent authority. These mechanical movements save me each and every time. After the session, I play Tetris. Shifting blocks in all directions, forming lines, filling gaps,… I fill my mind to erase invasive images. It helps tremendously, but every now and again, an image might slip back into my mind.

Main hurdles

- Not able to talk to someone: the nature of the work makes it challenging to talk about it to people outside the work field. Additionally, the high workload at Child Focus in general leaves little time and space to decompress.
- Risk of intrusive memories: the repetitive exposure to traumatic events may lead to involuntary memories, impacting individuals in the short, medium, and long term.
- Loss of focus after dealing with huge amounts of material and exposure to already actioned-known CSAM content.
- There are no scientific studies describing the short-term, mid-term, or long-term consequences or the overall impact.

Help us achieve our ambition

We aim to prioritize the well-being of our employees, and protect them as much as possible from short, middle and long term affects from exposure to violent content.

Challenge 4

Balancing different rights: between privacy and child protection. How can we better protect our children through legislation (national or EU), governance and/or software design (e.g. attribute-based encryption)?

EU policymakers appeal to the responsibility of **Service Provides to take risk mitigation measures and detect known and new sexual abuse material and grooming on their services (including E2EE).** Privacy advocacy groups argue fiercely against detection, and want to exclude interpersonal communication and E2EE from the scope of forthcoming legislation. This is a cause for concern, especially considering the increasing trend among major tech players to encrypt their chat services.

"Story of Aïda"

"Why Privacy and Protection should go hand in hand"

"Enticed on Discord, Aïda was led to WhatsApp, where she was persuaded to create intimate images of herself. Her perpetrator threatened to share them if she did not share more images. She contacted Child Focus. As Trusted, Flagger Child Focus e-mailed META with the details of the accounts and an urgent call to block the account. An automatic response came in return, stating that META is not allowed to gain access to the content of the chat due to privacy legislation. Two days later, Aïda's intimate images were disseminated."

Main hurdles

- While minors are increasingly more online and becoming targets for predators and advertisers, their voice, participation and protection are often not prioritized. How do we give them proper control over their online experience?
- The age of internet users is decreasing, with 8-year-olds now venturing online. How do we address these challenges posed for this young population?
- While the responsibility for online content and behaviour primarily falls on users, safety tools and applications have been developed to give parents and minors a semblance of control. While this seems promising at first glance, it should not absolve companies of their responsibilities.
- Despite the translation of many e-Privacy Directive rules into long 'terms and conditions' and cookie-preference clicks, the question remains: Are we truly in control of our data? Is 'informed consent' really possible?

Help us achieve our ambition(s)

We have various ideas for this challenge, and we'll determine the best approach or combination together during the hackathon.

- Assist us crafting a balanced multi-rights approach for policymakers in the realm of digital environments for children.
- Join us in envisioning an internet governance structure tailored for and by children.
- Collaborate with us in creating a technical rights tool that not only raises awareness but empowers children to actively demand their rights to privacy, information, and protection.

Challenge 5

New Threat Detection: How can we use technology to our advantage to identify and manage information on new threats?

Every day there are new trends, new challenges, new hypes going viral on social platforms. They require our full attention and our appropriate reaction, because they could contain risks to the integrity and wellbeing of our children.

“Hypes going viral”

“Have you ever heard of the blue whale challenge?”

The Blue Whale challenge, also known as the Blue Whale game, is a social media challenge that encourages children, teenagers and other users to complete specific challenges over the course of 50 days that are assigned to them by an anonymous “group administrator”. The challenges intensify as the game progresses. The last challenge and the only way to “win” is to die by suicide.

Main hurdles

- Staying ahead of any emerging threat poses the most significant challenge. Every report processed through our service has the potential to evolve into something more substantial. How can we know this beforehand? What methods can we employ to forecast its progression based on initial indicators?
- Centralizing and automating information: Currently, the Information-gathering process relies heavily on manual efforts, involving numerous emails, various documents and spreadsheets.
- Privacy concerns hinder the seamless sharing and exchange of data among experts.
- Ensuring everyone stays informed about developments, even internally, and establishing an effective early warning system proves challenging.

Help us achieve our ambition

Assist us in promptly detecting emerging threats, enabling us to issue timely warnings and safeguard children from potential harm.