Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Architecture and Design
Department of Design

Nakul Pathak

Building Effective Interactions

Making children aware and protecting their privacy in online environments

Master's thesis in Interaction Design
Supervisor: Professor Patrick Bours
Co-supervisor: Assistant Professor Giovanni Pignoni

June 2021

NTNU
Norwegian University of
Science and Technology

Nakul Pathak

Building Effective Interactions

Making children aware and protecting their privacy in online environments

Master's thesis in Interaction Design
Supervisor: Professor Patrick Bours
Co-supervisor: Assistant Professor Giovanni Pignoni
June 2021

Norwegian University of Science and Technology
Faculty of Architecture and Design
Department of Design

NTNU
Norwegian University of
Science and Technology

1 Preface

This master’s thesis is part of Master’s in Interaction Design programme at the Department of Design at NTNU in Gjøvik. The planning of research, literature review, potential challenges and steps were outlined in the autumn semester in 2020 through the course IMT4885 Research Project Planning. The actual research and analysis of the data was conducted in the spring semester in 2021. The research methods such as interviews, surveys and focus groups were conducted collaboratively with Marit Sylstad - a fellow master’s in Interaction Design student. The individual research questions were combined and some of the questions were kept common. The common questions were targeted towards understanding the demographics. The workload of the thesis corresponds to 30 ECTS. The work done is part of the AiBA project at Norwegian Biometry Laboratory at NTNU.

I have always been intrigued by technology’s role in human lives. I have been observing the lives around me and have realised that many things are around the technology surrounding us. It has impacted many areas of our lives. Even though, it has some huge benefits, it comes with its own disadvantages and risks. I was contemplating over different topics for my thesis in the summer of 2020, and I came across this topic. Having read about some of the worst crimes, I was curious to find out how can design help to prevent it from happening. I realised that choosing this topic will not only contribute to research knowledge but also can positively impact children’s and parents’ lives. It has potential to make a difference in people’s lives, irrespective of their location in this world.

At last, I hope this thesis helps the AiBA project and inspires the community of designers in some ways. The entire process has been a truly eye-opening experience. It has made me realise that human lives are way beyond boundaries of the digital world. That in itself is a complete and enriching experience.

- Nakul Pathak

2 Acknowledgement

This thesis would not have been possible without the help and support of a few wonderful individuals. I would like to take a moment to thank them all as follows –

First, I would like to thank my supervisor Patrick Bours for introducing me to this topic and providing an opportunity to work with AiBA project. I highly appreciate your strong support, trust and guidance throughout the process.

My co-supervisor – Giovanni Pignoni, for helping me through all the challenges, validate and ideate number of details throughout.

Huge thanks to Marit Sylstad – a fellow master's in Interaction Design student, for successful collaboration to conduct research and establishing collaboration with schools. It was really great working with you, to detail out all aspects of our research. The collaboration certainly helped to go a step further than what was possible.

Special thanks to Frode Volden for helping me with data analysis in SPSS. I have gained very useful and practical knowledge through our interactions.

This research would not have been possible without support from Kopperud Skole, and Vestre Toten Ungdomsskole and concerning staff members. Thank you for providing us an opportunity to conduct research and making it possible to establish contact with participants. Huge thanks go to all the participants who took time from their busy schedules to participate.

At last, thank you to all my fellow classmates for making this amazing and happening journey. I have learnt a lot from you all and enjoyed the times.

-Nakul Pathak

3 Abstract

With increased number of mobile phone users and chat applications, the advantages also bring along risks of using it. Children have been victim of sexual grooming and abuse. With increasing use of chat applications for various purposes, children are facing negative experiences online. Large number of studies have investigated grooming as a concept, processes involved and strategies to protect children. Despite these, the current accounts lack catering to privacy issues, support for child self-regulation, and ways to build awareness to tackle risks. The analysis of existing literature highlights that there is a lack of features that help children be self aware to handle different situations. This research takes a look at how design empowers children and parents to collaborate and communicate to solve these issues while preserving children's privacy. The research attempts to solve and understand whether simple interactions with an app or a digital platform can help to solve challenges and help children tackle risks. Well known methods from User Centred Design methodology such as interviews, surveys, focus groups are utilised to understand different aspects, nuances with parents and stakeholders. A low-fidelity prototype is created, tested and iterated further with designers and children through focus groups. The research was conducted with children and their parents from the schools around Gjøvik. Findings show that trust, communication, privacy and monitoring are key aspects involved around these issues. Children's interactions with an app or a system have potential to bring in the desired effects and build self-awareness. However, more testing is required to validate and fine tune the details of proposed solution to suit children's and parents' real-life usage. It is found that User Centred Design methodology has a potential to uncover challenges around these issues and can create a robust solution catering to dynamic aspects of it.

This thesis and research are conducted as a part of the AiBA project at NTNU in Gjøvik. The findings can be utilised to inform the future solutions in AiBA and by researchers working in these areas.

Table of Contents

4 List of figures

5 List of tables

6 Acronyms

DwI	Design with Intent
HCI	Human Computer Interaction
MVA	Minimum Viable Actions
NTNU	Norges Teknisk- Naturvitenskapelige Universitet
NSD	Norsk senter for forskningsdata
UCD	User Centred Design

1 Introduction

In recent years, conversations have taken different shapes and forms in everyone's life. The modes of communication have also changed drastically in the last two decades. In addition to face-to-face conversation, talking to someone over a digital platform using text, voice or video is one of the important modes of communication these days. The importance of this way of communication has increased extensively since the entire world started facing harsh implications of the covid-19 pandemic.

Along with adults, children too have started and have been using digital platforms to connect with people in their circles. When it comes to safety, there are unique set of challenges posed in front of all of us. Protecting children without minimizing or restricting the benefits of the digital platforms is of utmost importance.

The thesis will look into following areas – information security aspects related to children's usage of chat apps, communicating risk to children and parents, child's privacy and interaction design applied to derive solution to problems explored. The primary set of methods will be from User Centred Design (UCD) methodology with few additional methods from the design field (Gray, Brown and Macanufo, 2010; Tomitsch *et al.*, 2018).

This thesis is part of AiBA project (Author input Behaviour Analysis) (NTNU, No year). AiBA detects grooming and sees whether the profile description matches the parameters obtained from algorithm. With continuous monitoring, it can detect and notify suspicious behaviours to concerned parties. The future AiBA platform is intended for parents as well as moderators employed at company that owns the application. This reduces the number of fake profiles and makes the platform a safer place to be.

1.1 Motivation and Impact

Cyber grooming and predatory behaviour (paedophiles) are prevalent problems for online platforms. According to a study, one of the well-known grooming process can have stages such as – friendship forming, relationship forming, risk assessment, exclusivity, sexual stages (Black *et al.*, 2015). Although, all these stages may not be present and if present, can be re-visited multiple times. An offender tries to extract information by various small talk methods and being empathetic towards the target (Black *et al.*, 2015). These cases have potential to turn into physical abuse and harassment. Another recent study reports that there is increase in children meeting online (with known and unknown people) and prefer being online than meeting in person (Smahel *et al.*, 2020). The study also notes that there is an increase in negative experiences online as compared to before. This makes protecting children more important than ever.

Any effort made in making a child's online presence safe will have positive effects on children's well-being and it acts as the biggest motivation to solve problems in this area.

To tackle these problems from interaction design as a tool, it is well known and observed that users' interactions and exposure with digital platforms' influence their behaviour. Thus, carefully designed interactions can help to reduce potential risks and increase awareness. A certain behaviour can [be made to] occur if there is enough motivation, trigger and ability (Fogg, 2002). Another example is the DwI (Design with Intent) method, where a solution is typically aimed at influencing users' behaviour (Lockton, Harrison and Stanton, 2010). According to Tromp and Hekkert, solving problems that involve changing behaviours allows designers to reframe the problem in a way that reveals relations beyond just cause-effect (Tromp and Hekkert, 2019). Solutions or interventions for such problems can then take completely different approach with which different influencing factors can be unearthed (Tromp and Hekkert, 2019). For example, on one side of grooming there are children and parents who get affected and on other side person who grooms. The process or thoughts might have started way before the action has been taken. Thus, applying these methods and thinking of problems holistically will not only protect children but also help discover some issues about why this starts in the first place.

In addition, every child has different ways of using chat applications and looks at it in different ways. A child might talk to strangers (or known) people for different reasons and perceives the risk differently. Although not every single occurrence will be with dishonest intentions, it is required to warn and protect children and parents when it actually is. These personality nuances and family dynamics can be discovered in great detail with the help of research methods in User Centred Design (see figure 4) methodology.

Newer chat applications are innovating new ways to be in touch with people. All platforms view privacy and security in different ways, and some might be very vulnerable. For instance, on a number of social media platforms it is possible to send/receive messages from someone who is not in your contact list. In such cases, a design that makes users aware about potential dangers is extremely important.

The other emerging problems are detecting perpetrators and potential risks around children. Newer chat applications and social media platforms such as Telegram, Signal, WhatsApp are offering features such as encrypted chats and private profiles makes it even harder to detect potential threats (Cale *et al.*, 2021). Limited number of ways to verify a profile is also a problem as it allows a user to create fake profiles easily.

Cybergrooming could entail and fuel another giant problem of child sexual abuse material production. The TOR browser and darkweb add on to the existing complexities of anonymity and adds another challenge in CSAM content production, distribution etc. (Cale *et al.*, 2021). In addition, the creation of CSAM material and cyber grooming share couple of common characteristics (described in detail in Background chapter) – cognitive distortion, committing a sexual offence (Cale *et al.*, 2021). Thus, it cannot be denied that two are interlinked and one can be a reason for the other to occur. The systematic review of literature around CSAM content production by (Cale *et al.*, 2021) reports that the CSAM material in itself could also be held against children to blackmail and be used against children to groom and thereby produce more material.

At a larger level, this future solution has a potential to identify grooming or predatory behaviour against not only children but also adults, for example scams and rape threats. Though the context and scenarios are completely different, the base idea of influencing behaviours and making users aware of the risks is key common factor between them.

The answers and solutions to the questions have huge potential to make positive impact on a large, global scale.

The insights gathered from this research can also be looked at as valuable contribution to design research practices. Understanding users' behaviours and debunking dark patterns (Gray *et al.*, 2018) go hand in hand. As awareness increases, users can voice out their opinions against dark practices and limit creators from doing so.

1.2 Research questions

In order to design effective solution, the research question to be focused on is as follows –

> *Can we design effective interactions to introduce positive risk-aware behaviour in children and parents, that protects a child against grooming, while preserving child's privacy?*

This research question can be broken down into sub themes that can be explored and answered through planned research and existing literature available -

- RQ1 - How do parents monitor their activity online and chat apps usage?
- RQ2 – What do parents and children think about children's privacy in different contexts?
- RQ3 - Children's understanding about privacy when it comes to risky and non-risky scenarios
- RQ4 - How can the design help children and parents to initiate a conversation and collaboratively work on problems/situations?
- RQ5 - How can the design help a child to make him/her aware of the potential dangers and monitor and reflect on their own?

1.3 Contributions

The research methods such as interviews with parents, survey and children were conducted in collaboration with another fellow master's in Interaction Design student. The researchers combined questions related to individual topics and explored the problem space. A common set of questions were utilised to understand the target demographic better.

The findings of this research contribute to understand the role of interactions to make children aware of different risks. In order to understand, first the effectiveness of the interactions is evaluated with parents, stakeholders and children. The research also brings out some of the key factors involved in a parent-child relationship in the context of children's usage of social media platforms. The resulting prototype can be used to further develop new AiBA system that can be set up on parents' and children's devices.

The research also highlights that following the methods from User Centred Design methodology has a lot of advantages and potential. The methods are valuable to get a deeper understanding and enable researchers to gather critical aspects from all sides. The researchers can build empathy towards the intended audience. The thesis therefore addresses the challenges with a potential solution and provides a ground for future researchers to base their research on. The thesis emphasizes that interactions with apps and platforms need to be designed carefully as it affects all users in number of ways.

2 Background

This section gives an overview of existing research related to grooming, privacy and design theory that addresses potential solution space. The literature review is primarily narrative in nature, as it suits the topic best. The literature was searched using ACM (ACM, 2021) as primary database and Oria.no (library system and search engine at NTNU) as supporting source to find relevant literature. The search keywords and phrases are as follows –

- Search keywords – children's privacy, interaction design, design, grooming, cyber grooming, predators
- Search timeline – Jan 2015 to March 2021
- Search phrase - AllField:(design for privacy) AND AllField:(interaction design) AND AllField:(protecting children) AND AllField:(human computer interaction) from Jan 2015 to March 2021, Artefacts available selected, using ACM (ACM, 2021)
    - Total results – 85
- Search phrase - [All: grooming] AND [All: predators] AND [All: online]
    - Total results – 15

After retrieving the literature, it was evaluated by considering abstract, and relevance to this research. The selected articles were further analysed. The remaining articles are retrieved through literature cited in the selected literature.

2.1 AiBA Project

AiBA (NTNU, No year) can observe behaviour of a person in chatrooms or on social media. As shown in the figure 1, with analysis of typing-rhythm behaviour and content of the conversation, grooming and/or harassment can be detected. The system can also predict the age, gender of the person and build a profile. The conversations that appear as potential grooming or harassment will be flagged, and moderators can evaluate it further. AiBA can evaluate a conversation and flag it for being predatory by analysing less than 40 messages on average.

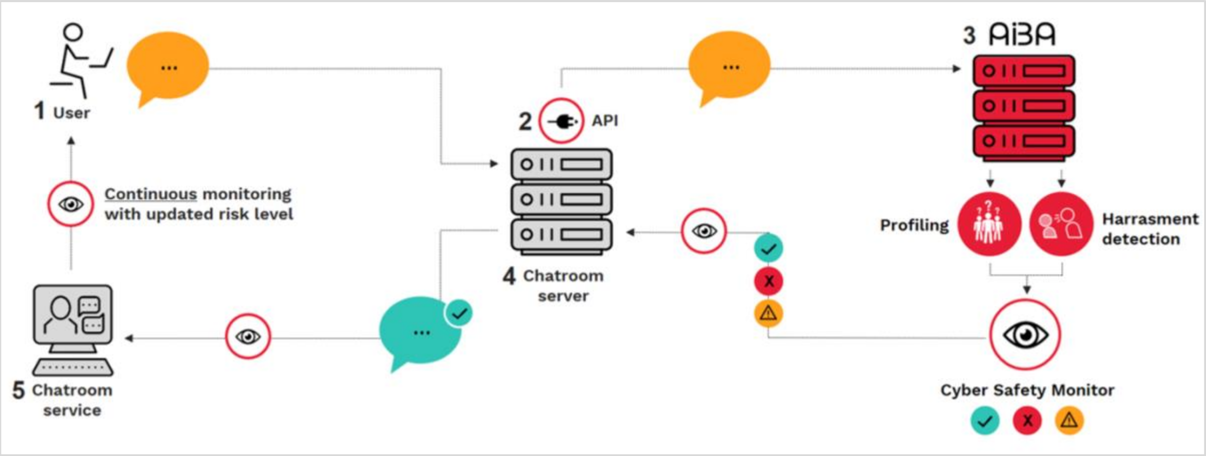


Figure 1 - AiBA ecosystem adapted from aiba.ai (NTNU, No year)

2.2 Grooming – Overview

2.2.1 Definitions

In order to understand finer nuances, it is necessary to look at what grooming is. In an article by Mladenović et al., the authors explored definitions across literature regarding cyberbullying, cyberaggression and cybergrooming. One definition as per the report is (Mladenović, Ošmjanski and Stanković, 2021) –

> *Child grooming is premediated behaviours intended for securing the trust of a minor, the first step toward future engagement in sexual conduct.*

According to the definition by (Gillespie, 2002), grooming is defined as follows -

> *The process by which a child is befriended by a would-be abuser in an attempt to gain the child's confidence and trust, enabling them to get the child to acquiesce to abusive activity. It is frequently a pre-requisite for an abuser to gain access to a child.*

Alternative definition for cyber grooming by (Gunawan *et al.*, 2016) is –

> *Online child grooming is defined as a process to approach, persuade and engage a child, the victim in sexual activity by using Internet as a medium.*

From (Meyer, 2015) grooming is called when there is an attempt of building a relationship that leads to a sexual relationship with a child by a paedophile.

Some of the definitions mentioned above do not use the word *paedophiles* (Craven, Brown and Gilchrist, 2006) as it is limiting. The term paedophile is ascribed to a being post a clinical analysis and may not apply to all of offenders (Craven, Brown and Gilchrist, 2006). According to Ward and Siegert's pathways model, psychological mechanisms such as emotional regulation, intimacy deficits, cognitive distortions and sexual arousal, all of these are involved for dysfunction (Ward and Siegert, 2002). Thus far, even though these studies have given the theory about grooming, it needs to consider all the events from start to the very end, rather than only reasoning behind it (Craven, Brown and Gilchrist, 2006). The authors (Craven, Brown and Gilchrist, 2006) also provide detailed stages of offence processes. Stage one starts at offenders' background, their perception about themselves and their life, stage five and six are planning and offending. At last, the stage nine that considers impact of these stages on offender's life. Mladenović et al. highlight that it is difficult to detect grooming as it starts with befriending the child (Mladenović, Ošmjanski and Stanković, 2021).

2.2.2 Grooming process

The existing literature has studied grooming processes in depth. There is some overlap between grooming process used in-person and online. Three types of sexual grooming have been identified, viz. self-grooming, grooming the environment and significant others and grooming the child (Craven, Brown and Gilchrist, 2006). It is necessary to have this understanding to prevent the child sexual abuse (Craven, Brown and Gilchrist, 2006).

According to the studies, the self-grooming phase starts with justification or resisting their own actions (Craven, Brown and Gilchrist, 2006; Van Dam, 2001). The authors point out that, offenders as well as non-offenders have maladaptive implicit theories. This establishes a connection to belief that strangers abuse more children than friends or family. Offender(s) might as well have an implicit theory that child seduced them, instead they abused the child (Craven, Brown and Gilchrist, 2006).

Second phase focuses on grooming the significant others and that might include parents, guardians and teachers. Offenders identify vulnerable children and try and be part of their social environment (Craven, Brown and Gilchrist, 2006). Van Dam maintains this with very detailed case studies where offender is well positioned in children's environments and also protected at times by adults involved (Van Dam, 2001). Offenders also target families with single parents and/or absent parents as this can enable them to be part of the environment (Craven, Brown and Gilchrist, 2006), however, this step in the process might be explicit or implicit. It is not that only children with dysfunctional or poor families are prone to grooming, all children are vulnerable in varying degrees (Lanning, 2018).

The third step in overall grooming process is grooming a child. Grooming a child could result into psychological or physical abuse. Physical grooming is moving the interaction/conversation towards sexualisation and psychological grooming is to make it more sexual (Craven, Brown and Gilchrist, 2006). Furthermore, Craven et al. state that "the child is groomed to want to be groomed" and offender can take this further by threatening or bribing to protect themselves and make the child responsible (or blamed) for all that has happened (Craven, Brown and Gilchrist, 2006).

Use of violence by molesters and/or offenders in grooming is lower than seduction (Lanning, 2005), as it entails chances of getting it discovered early (Lanning, 2018). A study interviewed victims and offenders from three different online grooming and contact sexual abuse cases. It pointed out that the grooming progressed through stages such as regular intense contact, deception, kindness and flattery, erratic temperament and nastiness, secrecy and grooming others (Whittle, Hamilton-Giachritsis and Beech, 2015).

Focusing on theme of this research and AiBA project, it is necessary to understand the grooming processes so that privacy issues could be placed in right areas. If the entire grooming process is imagined as a continuum of phases or steps, privacy issues could even be placed at the beginning of the process. Alternatively, privacy issues could also occur even before a child has been approached by a potential groomer.

2.2.3 Privacy and grooming

Privacy in general terms is ability to be anonymous and avoid having to disclose any information that identifies you as a person. Privacy can be looked at as a balance between desire for information disclosure and personal communication almost like cost-benefit relation (Kimmel, 1996) and privacy is of contextual nature (Sheehan, 2002). Factors such as situational forces, pressure from others, societal norms and the way it is monitored can shape privacy concerns (Kimmel, 1996). Very few studies investigate the effects of parents' and children's privacy perspectives on children's behaviour online (Wisniewski *et al.*, 2015, p. 304). A conceptual framework is provided by Wisnieswski et al. to understand privacy concerns, parental mediation strategies and teen privacy behaviours as shown in figure 2 (Wisniewski *et al.*, 2015, p. 306). Younger teens are likely to experience more direct intervention by parents (Wisniewski *et al.*, 2015).

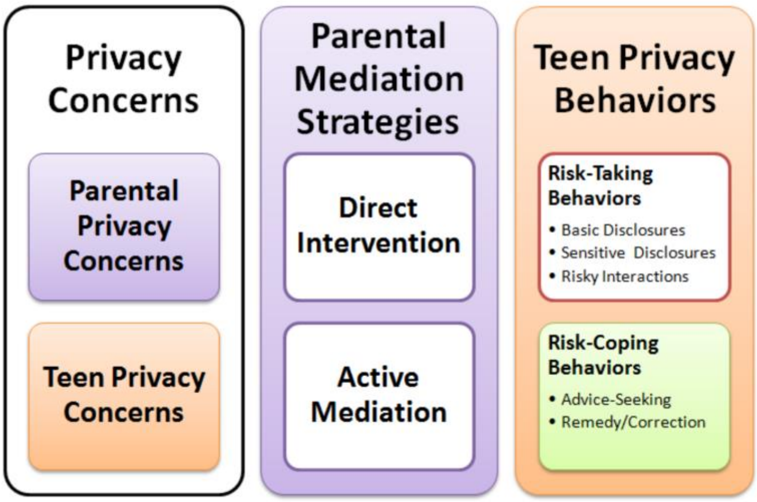


Figure 2 - A conceptual framework to understand privacy behaviours and parental mediation strategies (Wisniewski et al., 2015, p. 306)

The authors also maintain that restricting all the online experiences can inhibit child's developmental growth due to positive experiences online (Wisniewski *et al.*, 2015). Herein, direct parental mediation is defined as follows (Wisniewski *et al.*, 2015, p. 304)–

> *Direct parental intervention [is] through the use of parental controls and/or reading and setting up a teen's social media privacy settings for him or her.*

Active mediation is defined as follows (Wisniewski *et al.*, 2015, p. 304)-

> *Active mediation which includes parents talking with their teens about what they post, reviewing information teens post, and/or commenting or responding to posts made by their teens on Facebook.*

Coming back to protecting children from dangers online, there are a lot of technical solutions that one can adopt. These include having apps on child and/or parents' phone, having a service/platform specific mode (children own user profile and/or explicit content filter). The child's privacy needs to be considered irrespective whether potential grooming is involved.

The framework called TOSS (Teen Online Safety Strategies) (see figure 3) has been created by (Wisniewski *et al.*, 2017a), in the feature review of apps that promote child safety. Framework focuses on different parental control strategies and teen self-regulation strategies.

This framework is beneficial to understand how the problem of overall children's safety online can be addressed in different contexts (Wisniewski *et al.*, 2017a). Parental control strategies are monitoring, restriction and active mediation. Teen self-regulation strategies are self-monitoring, impulse control and risk coping. Surprisingly, the structured qualitative feature analysis by (Wisniewski *et al.*, 2017a) revealed that, out of 75 apps on android platform, 89% apps have designed for parental control. Only rest 11% of the apps are designed for teen self-regulation strategies.

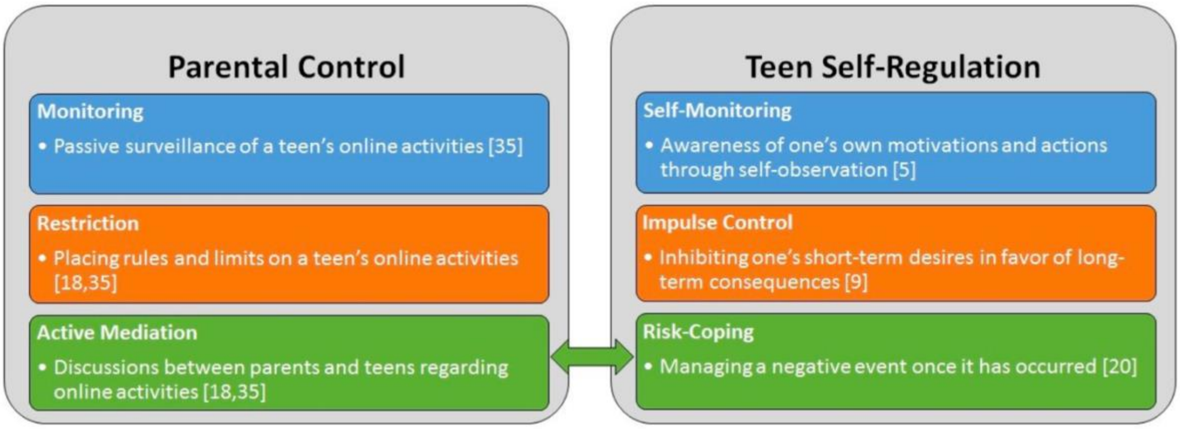

Parental Control
Monitoring
• Passive surveillance of a teen's online activities [35]
Restriction
• Placing rules and limits on a teen's online activities [18,35]
Active Mediation
• Discussions between parents and teens regarding online activities [18,35]
Teen Self-Regulation
Self-Monitoring
• Awareness of one's own motivations and actions through self-observation [5]
Impulse Control
• Inhibiting one's short-term desires in favor of long-term consequences [9]
Risk-Coping
• Managing a negative event once it has occurred [20]

Figure 3 - TOSS (Teen Online Safety Strategies) conceptual framework, adapted from (Wisniewski et al., 2017a)

Technical mediation is restrictive and very little research has been done to evaluate its effectiveness (Wisniewski *et al.*, 2017a). The authors state that monitoring and restriction are detrimental to trust between child and parent and potential to stifle his/her creativity through use of digital media and devices. The device may render itself as not-so-useful if excessive monitoring and restrictions are implemented. However, with the help of active mediation a child seeks help from parent(s) to deal with risks or incidences online, called "empowering effect" (Wisniewski *et al.*, 2015).

Existing solutions are in the form of an app that is installed on child's phone, being a ghost and tracking all possible information (Wisniewski *et al.*, 2017a). A companion app is installed on parents' phone to get detailed reports varying from browsing history, apps installed to collect tiniest usage detail such as content of text a message (Wisniewski *et al.*, 2017a). Throughout the analysis, it is apparent that privacy invasive monitoring and restriction are valued over self-regulation and all teen self-regulation tools are poorly supported in apps (Wisniewski *et al.*, 2017a). This can be backed up by another diary study findings of 68 teen-parent dyads, where researchers found that among all reports only 28% risk reports specified teens sharing details about what has happened (Wisniewski *et al.*, 2017b).

When it comes to online risks, it is debatable whether teens or children should be seen as equally capable for taking some decisions on their own. Nonetheless, children can be nudged in the direction of ideal (or close to ideal) behaviour by giving some insight with the help of raw data available from their smartphones (Wisniewski *et al.*, 2017a). Nudging is providing options to alter people's behaviour in predictable way without restricting any other options or causing significant gain or loss in terms of incentives (Tromp and Hekkert, 2019, p. 52). For example, screen usage time and warning about contacts that are not saved or lack information. Overall, it can be hard exercise to define the ideal behaviour as it is highly subjective and contextual to a family and a child.

On design side of apps, considerable usability issues have been identified (Wisniewski *et al.*, 2017a) that deteriorate the overall experience. Digital solutions also need to promote family values such as collaboratively working on these issues with children, trust and autonomy with care (Wisniewski *et al.*, 2017a, p. 534). In another study that conducted participatory design sessions with 12 children, the researchers found that children debated and resisted parents observing their entire conversations, however, involving them if need be (Badillo-Urquiola *et al.*, 2019).

Children also desired some level of privacy, autonomy and help to facilitate conversations with their parents (Badillo-Urquiola *et al.*, 2019).

2.3 Design methodologies

There are many existing methodologies that can help address the problems systematically (Baxter, Courage and Caine, 2015; Stickdorn *et al.*, 2018; Wendel, 2014; Dam and Teo, 2020). The four-stage model for designing for behaviour change depicts necessary steps to understand behaviours and actions of users (see figure 4) (Wendel, 2014).

Since it focuses mainly on behaviours, it may fail to understand nuances of users' environment, scenarios and the big picture in detail. User centred methodology can help to understand and fill in the gaps in knowledge about users.

Pinter et al. provide an insight through their literature review that interaction design in connection to children's safety online is not sufficiently addressed in the studies and literature (Pinter *et al.*, 2017, p. 352). Furthermore, the authors point out that mixed-method approaches are not utilised that often (Pinter *et al.*, 2017, p. 353).

All in all, design methodologies can support solutions that address factors such as –

- Fear-based paternalism (Pinter *et al.*, 2017, p. 354),
- Parent child communication, as it is superior to other mechanisms (Pinter *et al.*, 2017)
- Self-awareness and risk coping (Pinter *et al.*, 2017; Wisniewski *et al.*, 2017a)

The design methodologies are inherently capable of capturing all aspects of problem(s) and deliver a well-rounded solution. Pinter et al. support that more studies need to adapt and "diversify our ways of knowing" (Pinter *et al.*, 2017, p. 355). This is interpreted as to have different sources of data to inform the solution and actions.

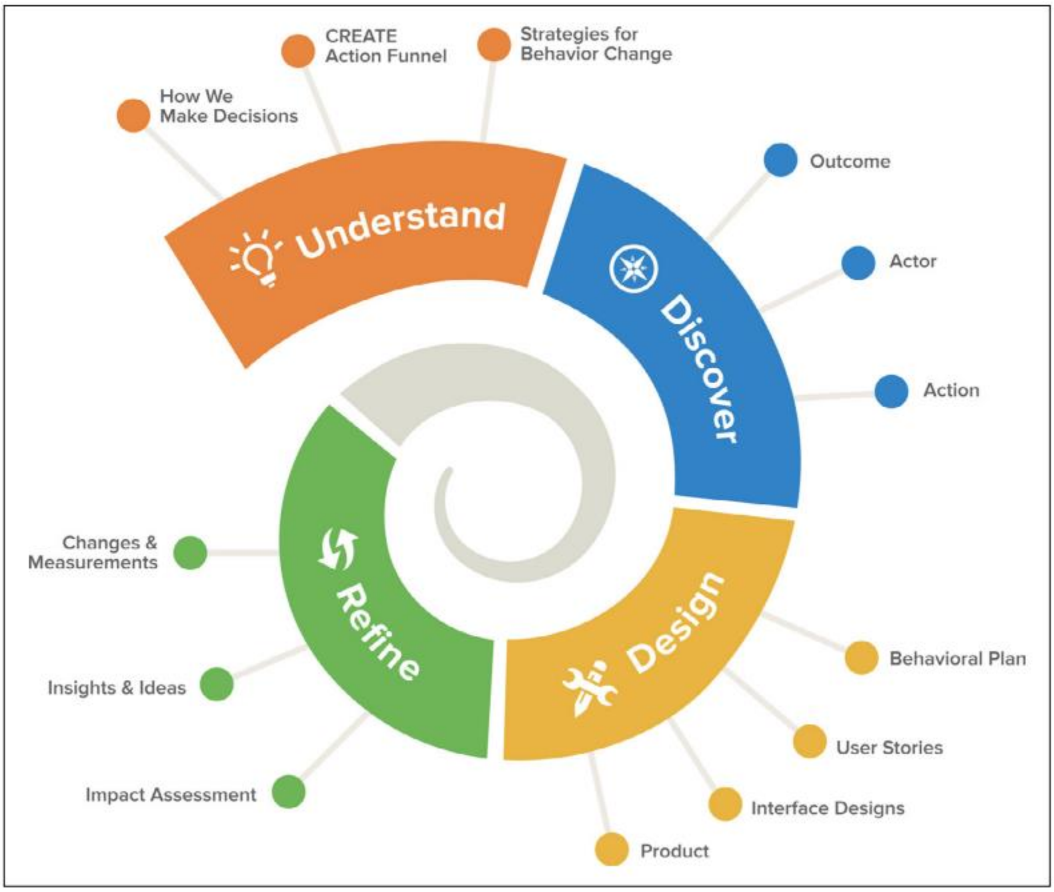


Figure 4 - Designing for behaviour change, adapted from (Wendel, 2014)

UCD methodology has been well established for many years (Baxter, Courage and Caine, 2015) (see figure 5). The tools and methods from the methodology have been practiced in variety of domains and applied to vast human-centric problems. Hence combining UCD methodology and four stage behaviour methodology have potential to bring best solution possible. UCD methodology has characteristic of being highly iterative, which can be seen as a potential limitation to this research, however, it can be solved up to certain extent by taking the solution to desired quality.

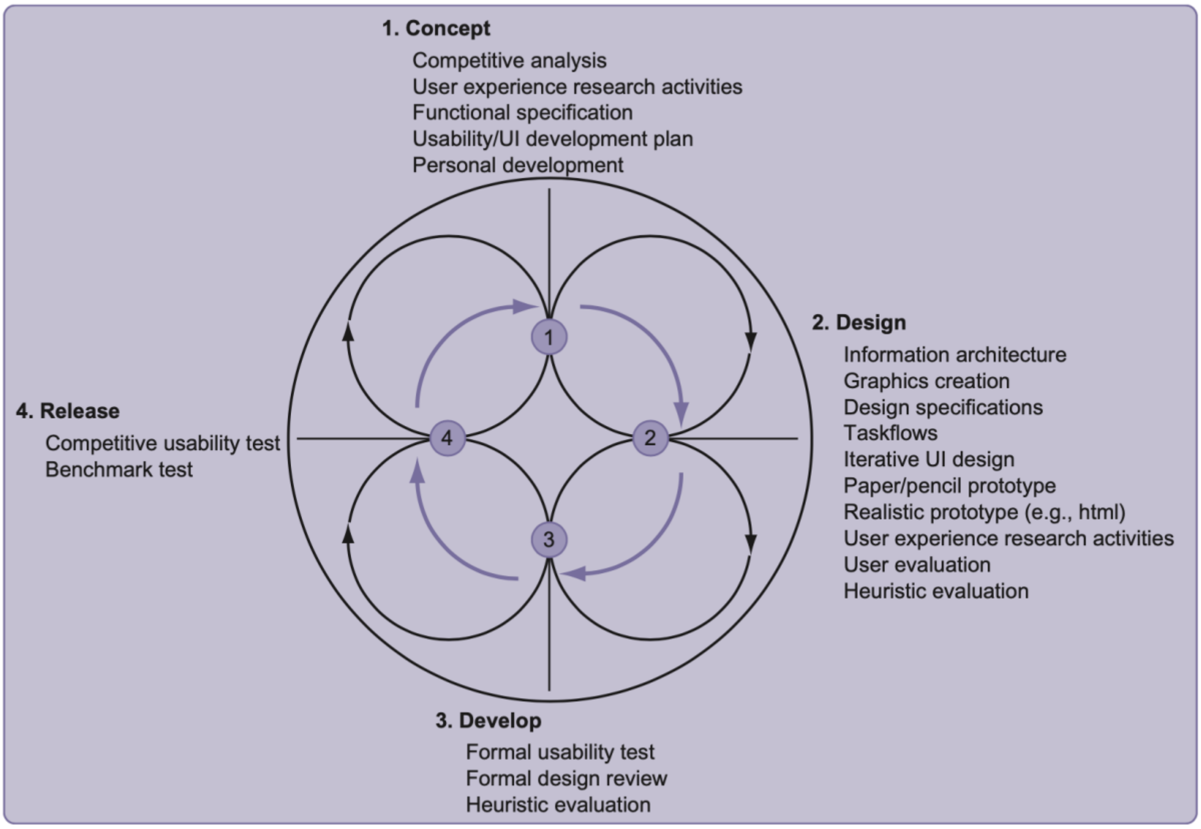


Figure 5 - User Centred Design methodology, adapted from (Baxter et al., 2015)

On the project level, the AiBA solution, is highly effective against detection of grooming risks, flagging fake profiles, predators and so on. According to the framework by Pinter et al., it falls under "Detection" and "Mitigation" (see figure 6). As children's awareness increases, the future solutions and versions of AiBA (and efforts to uncover different approaches) that address the points mentioned above, will strengthen the "Prevention" side of it (Pinter *et al.*, 2017), as shown in figure 6.

2.4 Design for privacy

Privacy is important for children as it allows them to take decisions, build relationships and also experience both positive and negative outcomes (Kumar *et al.*, 2018). Kumar et al., give an example of sharing location with a large group. By doing this, range of outcomes are possible, such as someone might break in or a personal information is shared to someone who does not need to know (Kumar *et al.*, 2018). Understanding these outcomes is important and that is not only limited to minimizing risks but also to minimize discomfort (Kumar *et al.*, 2018). Wisniewski et al. identify the need to have more sophisticated mechanisms to detect a child's privacy issues that are less visible to parents (Wisniewski *et al.*, 2015). Online safety software needs to draw attention to hidden privacy risks to encourage voluntary risk-coping and also need to educate parents of new technologies and associated risks (Wisniewski *et al.*, 2015). Traditionally Human Computer Interaction (HCI) methodology or User Centred Design methodology has been used to investigate privacy and relevant dimensions in various fields. One concerning literature review (Wong and Mulligan, 2019, p. 5-6) highlights design being used in three different ways – 1) to inform or support privacy, 2) to explore people and situations, and 3) to critique, speculate or present critical alternatives. According to the review results the second and third dimensions are underused.

Design provides a way to understand relationships between actors, stakeholders and helps to reflect upon situation and context (Wong and Mulligan, 2019). Thus, it is important to explore in these directions with a variety of UCD methodology tools at hand.

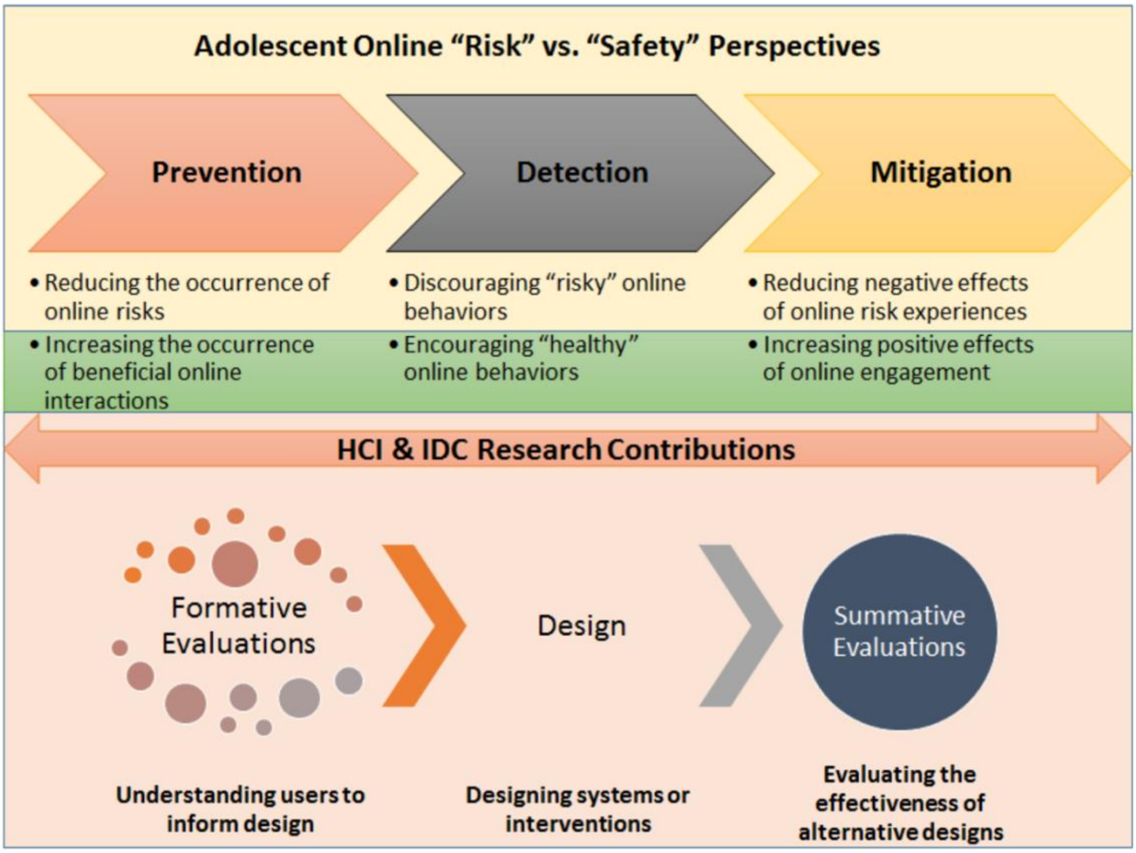

Adolescent Online "Risk" vs. "Safety" Perspectives
Prevention
Detection
Mitigation
• Reducing the occurrence of online risks
• Discouraging "risky" online behaviors
• Reducing negative effects of online risk experiences
• Increasing the occurrence of beneficial online interactions
• Encouraging "healthy" online behaviors
• Increasing positive effects of online engagement
HCI & IDC Research Contributions
Formative Evaluations
Design
Summative Evaluations
Understanding users to inform design
Designing systems or interventions
Evaluating the effectiveness of alternative designs

Figure 6 - A framework that represents contributions from existing literature, by (Pinter et al., 2017, p. 355)

As stated before, design plays an important role in facilitating communication between children and parents. Therefore, not only the underlying concept solution is important, but also the journey that a parent/child takes right from finding the app, setting it up and getting benefits out of it.

In this case, design can have multiple goals such as empowering children and parents in following ways–

- Increase children's and parents' awareness about potential dangers
- Participate in collaborative healthy communication, whether risk or no-risk situations
- Promote and establish healthy habits of self-evaluations and monitoring (for children)
- Provide insights from data that is already available on smartphone. For instance, screen time, trusted/added contacts

All of these goals translate differently to actual components in design/interface, some may not even need an actual real estate on screen and can merely be supported by combination of words and layout. On the contrary, while designing these intervening interfaces, designer needs to be aware and critical of overall outcome of apps. Chat apps are targeted towards a wide population, and it might have different goals in the product development roadmap. Protecting children is a part of it for some of the apps, at least. To achieve higher adoption rates and value for users, (Wendel, 2014) advises to identify Minimum Viable Actions (MVA) that outlines what the app really needs to achieve. This might mean mapping actions on interfaces for all scenarios and severity.

To design the concepts, (Wendel, 2014) describes three targets and phases of design –

- Structuring the action
    - Set of simple and easy steps that users can understand and act on, get rewards
- Design the environment
    - Understanding distractions, providing cues and motivating users
- Prepare the user
    - Giving sufficient information to users to act, educating them and establishing associations between their likes and actions

Another way to look at actions is with *CREATE action funnel* (Wendel, 2014). For an action to be taken, it needs to go through phases such as Cue, Reaction, Evaluation, Ability, Timing, Execute action and users can drop out of the flow from any of these phases (Wendel, 2014, p.40). CREATE action funnel and task flow (Baxter, Courage and Caine, 2015) can be collectively used to understand the flow, to debug and test solutions.

To persuade users to get habitual to some of the routines, psychology theories can be integrated with design. Understanding beliefs at play is important while addressing a behaviour that is supposed to happen. A particular behaviour has three beliefs behind it, behavioural outcome belief, normative belief, control belief (Wendel, 2014; Yocco, 2016). Here the behavioural outcome belief is where a child is concerned about of their actions, and it is highly subjective for the child, family, etc. Normative belief can be addressed through mechanisms such as reviews, ratings, experiences of fellow children and/or parents after using the platform or just word of mouth publicity.

This will normalize the use of such systems and instil an opinion that having such system to protect and help have a conversation. As far as control belief goes, giving both parents and children control over their actions might increase their buy-in, resulting in higher adoption rates. Overall design outcome needs to highlight the positive side and provide valuable, usable solution to the users (Yocco, 2016; Wendel, 2014).

Understanding the decision-making process and heuristics that go behind every decision will help understanding which decisions are favoured. Users often establish reference points to determine gain or loss in relation to a decision (Yocco, 2016). Knowing these reference points is key as it can help to know where children need to ask for help, what actions children and parents can take. For the resulting interface to be clear and easy to understand it is essential to map decisions, decision points frequency of making decisions to interface and roles. Continuing further, for children and parents dealing with these sensitive issues is likely to lie in unfamiliar or semi-familiar region in the spectrum of thinking interventions (Wendel, 2014, p. 22). Hence target behaviour can be designed to lie around semi-familiar and eventually very-familiar regions. (Yocco, 2016) advocates considering behaviour of only those who are in charge of decision making, fails to specify scenarios when it should not be done.

Alternatively, Fogg’s behaviour model is insightful to persuade users (Fogg, 2002; Fogg, 2009). It highlights, with enough motivation, right trigger and ability, a behaviour can be made to occur. Limitations could be to measure ability and motivation, as it is highly subjective, and motivation could be missing as some might be unaware or do not feel the need to act or do not have ability to act. In addition, multiple factors can be in the way and might prevent users from taking an action, such as limited attention span, distrust in app/product, fear of failure and missing urgency (Wendel, 2014).

2.4.1 Designing and testing the interface

The concrete knowledge of parents' and children's situations, contexts and environment can be gathered using surveys, interviews, contextual enquiry, personas, journey mapping.

To move from data analysis to concrete interface designs, both of the design methodologies provide a range of methods. These include from designing low fidelity prototyping, paper prototyping/sketching, high fidelity mockups to testing with usability heuristic evaluation, usability studies, A/B testing, and so on (Wendel, 2014; Tomitsch *et al.*, 2018). More details regarding these methods are specified in methods section.

As far as visual design of the product is concerned, the solution might need to follow brand's that is AiBA's visual styles. According to the researchers of a study, colours with higher colour heat and activity are preferred by participants and also more trustworthy in an interface (Ou *et al.*, 2004b; 2004a). The visual design also needs to cater to children's understanding of icons, interface elements, gestures and clear, unambiguous notification when parents are monitoring them or going through the data (Badillo-Urquiola *et al.*, 2019).

2.5 Indicators in existing social media

Current social media apps provide some indicators that help users to identify and understand a user's own privacy. For example, in Instagram, if someone who is not in a user's contacts/follower list sends a message (direct messaging), it appears as a message request (Laffey, 2020). Upon opening, there are options to ignore the message, block or report the account/user as shown in figure 7. In TikTok, direct messaging can be turned off completely or can be done only when two people follow each other (Tiktok, 2021). However, it is possible to comment and then eventually follow a user and message. For children, these settings stay the same with some modifications and default restrictions (Tiktok, 2021).

Similarly, Facebook (Zuckerberg, 2020) provides privacy check or reminders after certain time period in users' feed, as shown in figure 8. Google also provides similar type of solutions to go through account and privacy settings across Google's services.

Thus, it is common to have service providers enable user to protect themselves from who can find them or who can see their posts. However, it lacks to provide an insight or actionable component to increase awareness and/or prevent risks. This is confirmed by the literature review done by Pinter et al., where they argue that design interventions as a solution for adolescent online safety have not been evaluated or explored enough (Pinter *et al.*, 2017). These approaches – "abstinence-only" as (Pinter *et al.*, 2017) calls it, only tackle the problem from reaching to children and not helping them to take any action. Therefore, it can result into critical problematic situations such as reducing overall productivity, effectiveness of the devices, unable to cope with risks. Pinter et al. further argue that children cannot learn, resolve or reflect on their experiences to cope up with new situations (Pinter *et al.*, 2017). However, some of the findings from the literature review conflict with another study that studies features offered by parental-control and adolescent/teen safety applications (Wisniewski *et al.*, 2017a). The reason for this conflict could be attributed to less coverage of apps, incomplete or insufficient documentation, awareness about solutions and coverage by researchers.

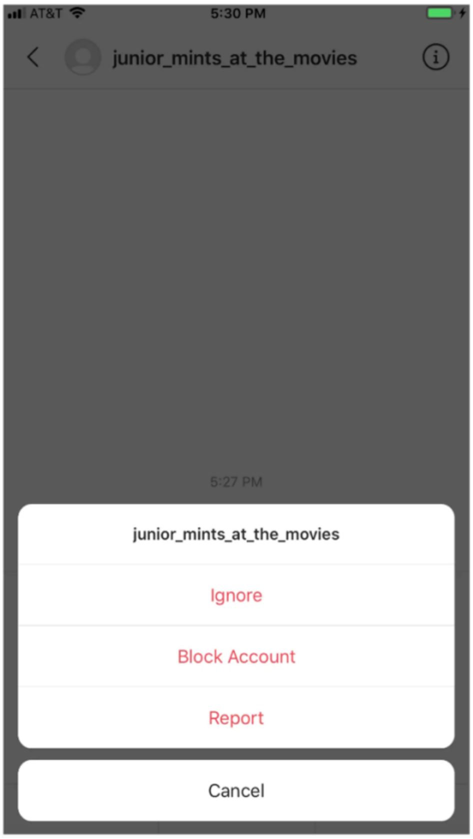
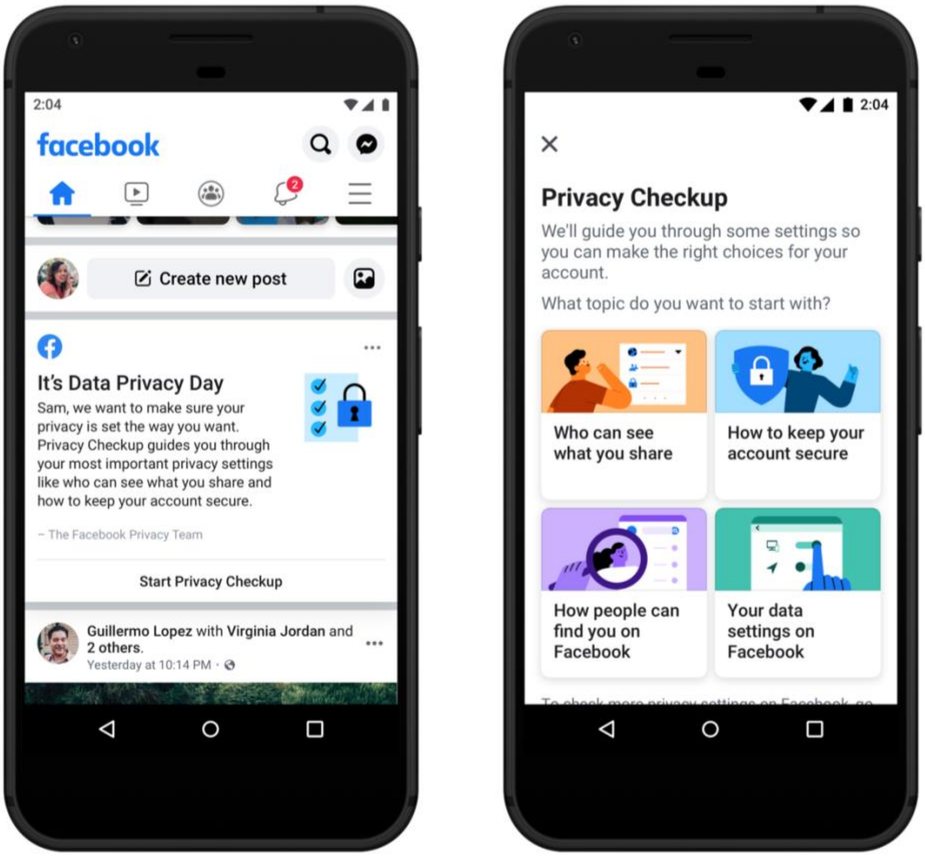


Figure 7 – Message request on Instagram



2:04

facebook

Create new post

It's Data Privacy Day

Sam, we want to make sure your privacy is set the way you want. Privacy Checkup guides you through your most important privacy settings like who can see what you share and how to keep your account secure.

– The Facebook Privacy Team

Start Privacy Checkup

Guillermo Lopez with Virginia Jordan and 2 others.

Yesterday at 10:14 PM ·

2:04

Privacy Checkup

We'll guide you through some settings so you can make the right choices for your account.

What topic do you want to start with?

Who can see what you share

How to keep your account secure

How people can find you on Facebook

Your data settings on Facebook

Figure 8 – Facebook's privacy check-up on phone app

2.6 Design interventions

Livingstone and Smith suggest that newer interventions that are targeted towards right population, that highlight best practices, and learn from mistakes are much needed and are under developed (Livingstone and Smith, 2014). The privacy check-ups mentioned above could be termed as design interventions that help achieve certain things. However, those seem to be generic and not theme-specific for this research.

One such intervention, inspired by the privacy check-ups, could be certain reminders that children see periodically. Children are nudged to go through risk-prone areas in their chat apps or in a dedicated app. Such solution can often be combined with notifications on smartphones or any digital devices.

Even though everyone perceives privacy differently, this solution can promote privacy awareness and users are likely to think and act on it. However, the case changes when children are using a solution. This research attempts to explore and see how different solutions perform.

Notifications are very important part of the users' interaction with smartphones and other digital devices. As far as messaging apps' notification go, studies indicate that users are attentive to notifications and respond to them quickly, usually within few minutes (Pielot, Vradi and Park, 2018; Pielot *et al.*, 2014; Dingler and Pielot, 2015). These notifications fall under Cue in CREATE action funnel (Wendel, 2014). Based on the framework developed by (Aranda, Ali-Hasan and Baig, 2016), notifications to nudge children in right direction can be designed to be in VIP quadrant as shown in figure 9.

Too many notifications at wrong timings can feel like "Nagging" (see figure 9). For notifications to be perceived important and worthy of users' attention, content and relevance at that point in time is also important.

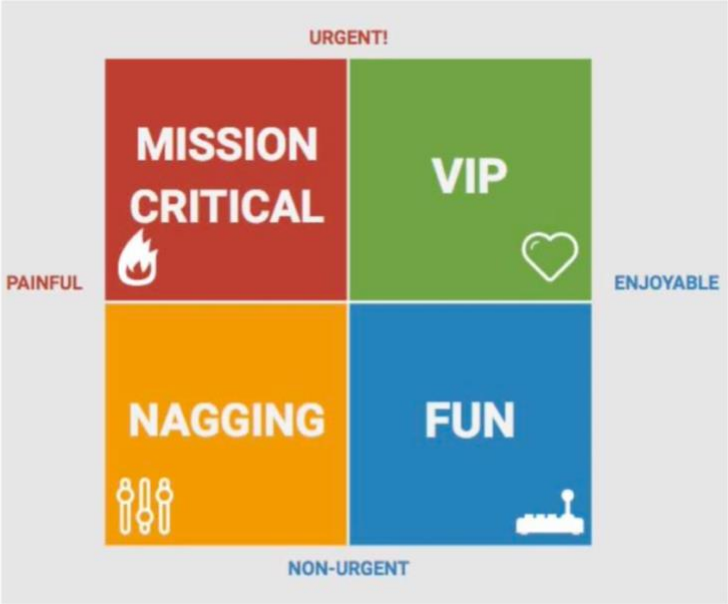


Figure 9 – Notification framework provided by (Aranda, Ali-Hasan and Baig, 2016)

To summarize, there have been many studies that focus on grooming strategies, reasons and processes behind it. However, the existing accounts lack to address issues of privacy and issues surrounding children's autonomy in sensitive issues. On the design side of it, literature on psychological models and design can be leveraged to gather insights. Mixed method approaches, design interventions that support child autonomy, risk-coping are less explored. Therefore, the key problems are required to be explored at different levels and through different sources. One such solution i.e., interaction could reminder as the privacy check-up mechanisms.

3 Methods

The thesis would continue to build on research that has been done previously by researchers that were part of the AiBA project. Since the theme of this project revolves around protecting children, it is important for researchers to know more about their lives and thinking in this setting. It allows researchers and stakeholders to build empathy towards children and their parents. In addition, preserving and conveying different contexts involved in the child's world is crucial to identify flaws with current ecosystems and thereby to build effective solutions. One of the main reasons behind this is to make the solution as effective as possible without crossing any boundaries. According to (Powell *et al.*, 2018, p. 648) -

> *Three issues create a concern about sensitivity: first, issues considered private, stressful or sacred, such as sexuality or death; second, issues that if revealed might cause stigmatisation or fear, such as illegal behaviour; and third, issues related to the presence of a political threat where researchers may study areas subject to controversy or social conflict.*

This text highlights critical areas that might have an effect on a child's thinking and behaviour in the future. The research also mentions that sensitive topics also depend highly on culture, families and societies and differences in raising children. It is highly contextual (Powell *et al.*, 2018).

3.1 Purpose and methodology

The goal of this research is not to make the children go through scary and uncomfortable imaginations but to understand their current ways of using technology, applications/software and their thoughts about these issues. The aim is to understand context and scenarios - both normal and problematic, that children and parents are part of. Every child is different and can potentially have different perspective with respect to privacy within a family and towards the outside world. Their ways of thinking are highly valuable and can prevent potential flaws in the solution being designed. The research can be roughly divided into 4 different well-known phases based on User Centred Design methodology – Research, Define and Ideate, Prototype, and Test (Baxter, Courage and Caine, 2015). The phases can be revisited and usually overlap. In addition, methods described can be part of one or more phases, as working in an iterative manner can yield better results. Although, nature and extent of these methods might differ. The following sub-sections present an overview of methods that are employed in respective phases.

3.2 Methods overview

The research follows User Centred Design methodology's (Baxter, Courage and Caine, 2015) phases in an iterative manner. Initially the research started with mapping out key problem areas with the help of current literature. After scoping down problems and research direction, interviews with stakeholders and parents were conducted. This was followed by survey for children, focus group with children and designers. The term "stakeholder" here refers to all the primary decision makers directly and indirectly involved in the development of AiBA system, which in this case are AiBA project team members and police officers. The details are shown in figure 10.

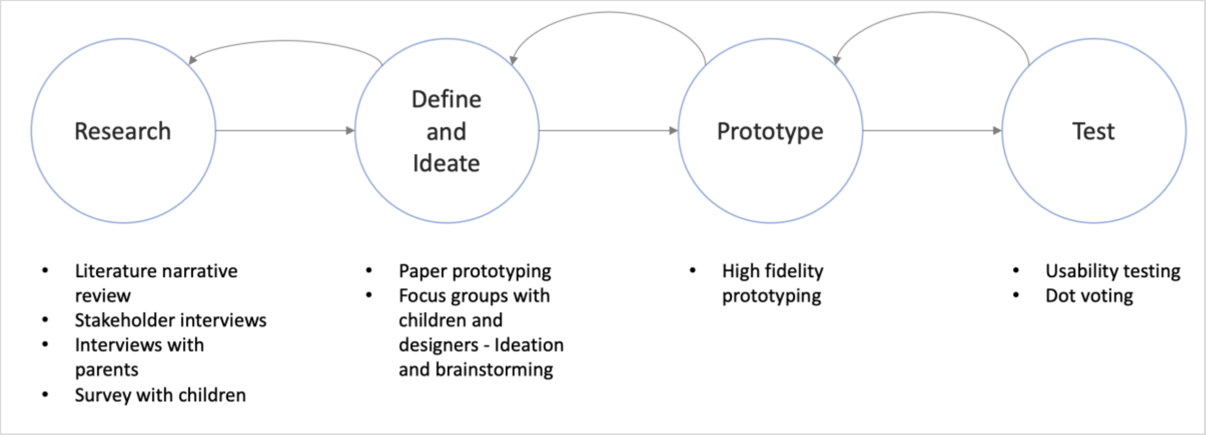

Research
Define and Ideate
Prototype
Test
• Literature narrative review
• Stakeholder interviews
• Interviews with parents
• Survey with children
• Paper prototyping
• Focus groups with children and designers - Ideation and brainstorming
• High fidelity prototyping
• Usability testing
• Dot voting

Figure 10 – Methods overview and phases in the research

The data and general observations from the previous research activities helped to set correct directions for upcoming research activities. The AiBA project has been collaborating with local schools in and around Gjøvik municipality for research purposes. In this case, teachers and schools act as gatekeepers and play an important role in providing access to children for research (Emmel *et al.*, 2017). For the research activities, three schools namely – Blomhaug Barneskolen, Kopperud Skole, Vestre Toten ungdomsskole (VTu) were targeted. Due to Covid-19 restrictions, Blomhaug Barneskolen could not participate in the research. Thus, respective school staff members from the other two schools were contacted to get access to children and their parents.

The target group included children from 5th to 9th grades (~9-15 years old) and their parents. This group was selected as –

- Children below 5th grade (less than 9 years old) might be too young to participate
- They are likely to have some restrictions around usage of devices and social media
- As per NSD, children between 16-18 years can consent by themselves. Maintaining and tracking this would have been an additional overhead on schools and could have affected research timeline.

Given the sensitive nature of the topic, to gather relevant necessary personal data, an approval from Norsk Senter for Forskningsdata (NSD) was requested at the beginning of the study. The research was done after getting an approval from NSD. The school staff members helped to share the invitation to participate in research activities on the school's internal communication system. The information gathered specific to a method is described further below.

3.3 Research

One can take different approaches to select the type of data to be gathered and methods to gather it. One way is to get qualitative data and capture insights in the form of user stories. For example, by using an online ethnography study (Stickdorn *et al.*, 2018) followed by interviews. Alternatively, quantitative data can voice out opinions of larger audiences, perhaps gathered using a survey. Choosing either of these might end up losing important data and thus a combination of these two is necessary. Such a hybrid approach is called "mixed-method designs" (Leedy and Ormrod, 2015). Since privacy in relation to chat applications and grooming is highly contextual, it is necessary to understand the scenarios children and parents are going to be in. In non-dangerous situations, it is likely that privacy would be ignored and may not get any attention. At the same time, for a solution to work for all children, quantitative data is also required to support insights from qualitative data.

Surveys and interviews are well known tools for assessing the scenarios involved. Questionnaire for semi-structured interview can be designed in such a way that allows probing the participants further whenever necessary. Hence it is possible to capture highly subjective experiences and scenarios from participants. Qualitative data can also be as trustworthy as quantitative data, and can possess high reliability and validity (Nowell *et al.*, 2017).

Research methods that were conducted as a joint activity with another master's student working with AiBA are as follows –

- Interview with parents
- Surveys with children
- Focus group with children

Rest of the research activities (stakeholder interviews, focus group with designers) were not conducted in collaboration. The thesis topics and directions were independent and collaborating for research helped to make the best out of participants' time. Thus, the resulting questionnaire for interview, survey and focus groups questionnaire were combination of 1) topics and questions that individual researchers were after and 2) some common demographic information that can be utilised by both researchers to inform their solution.

3.3.1 Interviews

Semi-structured interviews with parents and stakeholders were chosen as an initial research method. Reasons to select interview as an initial method are that 1) interviews yield rich qualitative data (Tomitsch *et al.*, 2018), 2) to get some additional feedback and 3) getting a richer understanding of children's world and contexts they are involved in. In addition, it can help to set the survey questionnaire's tone right and make it comfortable to ask and answer. Teachers are an important part of this as well, as they are involved in educating and making children aware about dangers involved. Teachers being key entity in children's lives, it would be interesting to understand how they make children aware of risks and good practices when using chat applications. However, their role in this research was limited due to scope and timeline constraints.

3.3.1.1 Interviews with stakeholders

The interviews with stakeholders were structured in three different parts. First part was about briefing them about the project, privacy and confidentiality details. Second part was about warm up questions that were intended to understand what their role and work is. And at last, the third part, were main questions which were aimed at knowing –

- Long term vision of AiBA as a comprehensive solution
- How stakeholders envision development and growth of AiBA
- Their understanding about intricacies involved in parent-children interaction on use of chat apps and grooming

- Their experiences in different cases and campaigns over the past few years in service

The questionnaire was slightly tweaked to suit both stakeholders who are actively working with AiBA and the ones that could use and/or contribute to AiBA in near future. According to the initial plan, stakeholders were not part of the research. However, understanding their challenges and perspectives about problem was necessary to tackle problem solution from all the sides. Therefore, key stakeholders that are part of the AiBA project were invited for a semi-structured interview. Other than the AiBA project team, 2 officers from the Norwegian Police department and an executive from a company that has social app for children, were invited to participate.

The stakeholder interviews were scheduled for approximately 30-45 minutes and were conducted online using Microsoft Teams. The complete questionnaire is attached in appendix 8.1.

3.3.1.2 Interviews with parents

Same as stakeholder interviews, the interviews with parents were structured in 3 different parts. The first and second part being about briefing them about the project, re-visiting confidentiality and privacy part, and ice breaker questions. The difference was in main questions that was further divided into 4 different parts, each of them focusing on different target areas. Questions in those areas were targeted to know more about -

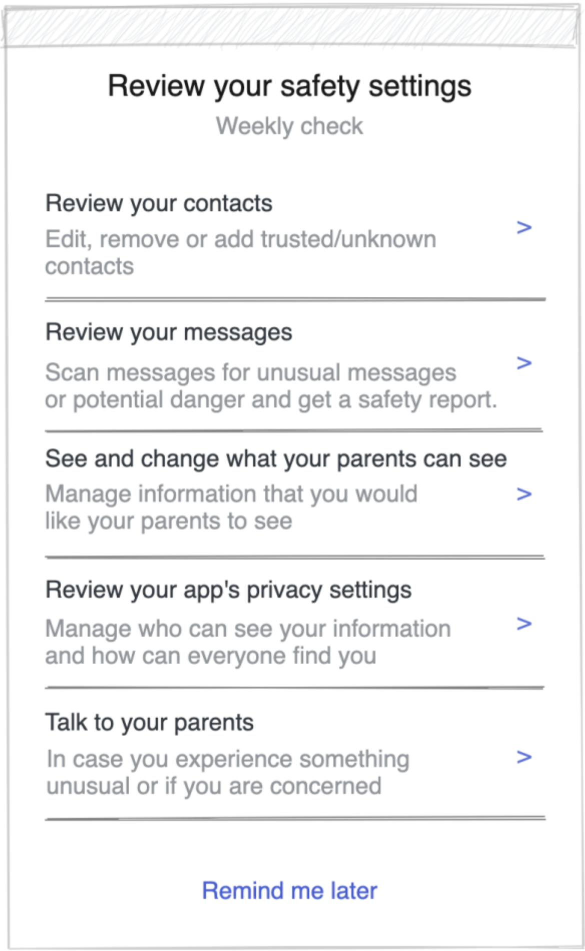
- Parents' understanding about children's privacy
- How parents prefer receiving information about grooming and related topics
- How parents use devices and social media, their awareness and challenges around the topic
- Digital solutions that parent use to ensure child's safety online
    - Challenges faced while using such digital solutions. For example, an app that monitors apps on child's device and sends permission when trying to install new apps

Before the research began, certain assumptions were made based on existing literature and individual understanding of the topic -

1. Most parents use some kind of parental control or monitoring tool. This means that parents monitor their child(ren)'s usage in day-to-day life.
2. Privacy can mean two different things – a) limiting who can see a child's profile, information, and account secure through settings in an app and b) privacy when parents are monitoring a child irrespective of potential grooming.
3. Parents would desire maximum control and prefer to get as much information as possible, when there is a potential risk.

The target population here is parents of children between 5th to 9th grade and from the schools mentioned above. The interviews were semi-structured and were scheduled for approximately 45-60 minutes. All parents were invited through a survey that had a brief description about the research and a form for them to sign up. Parents who signed up, were then followed up with a consent document drafted according to NSD guidelines and a link to book a timeslot for meeting. Due to ongoing Covid-19 situation, all the interviews were conducted online over Microsoft teams meeting. For the analysis purposes, interview's audio was recorded through the Dictaphone app. Parents were given a choice to answer questions either in English or in Norwegian. All the participants were also given a choice to say no to the recording and can skip a question, if they felt uncomfortable or did not wish to answer. The detailed questionnaire is attached in appendix 8.2.

Another key part in interviews with stakeholders and parents was prototype's usability testing. A low-fidelity prototype was tested as a proof of concept. The prototype was created using Excalidraw, an open source, virtual collaborative whiteboarding tool. Participants were given a short description about the purpose of the prototype before actually showing it. Afterwards, the prototype was shown on the screen to understand their overall feedback, expectations from the solution. The prototype is shown in figure 11.



Review your safety settings

Weekly check

Review your contacts

Edit, remove or add trusted/unknown contacts >

Review your messages

Scan messages for unusual messages or potential danger and get a safety report. >

See and change what your parents can see

Manage information that you would like your parents to see >

Review your app's privacy settings

Manage who can see your information and how can everyone find you >

Talk to your parents

In case you experience something unusual or if you are concerned >

Remind me later

Figure 11 – Low fidelity prototype for usability testing

3.3.2 Surveys

Surveys can help getting quantitative data from the research (Tomitsch *et al.*, 2018). Surveys are selected as a key method as it is effective in getting data from large number of audiences. Existing literature relating to the topic also highlights that self-reporting methods are used successfully in the studies. A literature review done by Pinter et al. found out that 83% of studies relied on self-report data by children and teens (pp. 353, Pinter *et al.*, 2017). The inherent issues involved in survey as a method can be counteracted by employing other methods and having a large sample size. Having methods such as interviews, focus groups which are used less, can potentially unearth newer directions to explore. The context was set based on the discussions with parents and stakeholders, and minor updates were made to the survey questions.

The survey focused on the following areas -

- Basic demographic information
- What apps (games, social media etc.) and devices they use, frequency of usage
- How frequently children meet someone who they got to know online, their experiences
- What personal information pieces they share with their contacts?
- Their awareness about using apps, being secure online
- Parent-child communication about issues they face online
- Their feedback on the features in the low fidelity prototype

The survey was kept simple to answer and understand. A pilot test was conducted on a 14-year-old girl to verify whether all the questions are understandable. Some questions were re-worded to convey precise meaning. Most questions were Likert scale questions. Survey was divided into multiple smaller sections to make it less overwhelming. Both English and Norwegian versions of the survey were created. The survey did not collect any personal data and children were ensured that their responses were not shared with their friends, teachers and parents. Initially the link to the survey was shared with parents to get their consent, before children saw the survey. After getting their consent, the schools circulated the survey link to children, using their internal communication system. Even though parents gave their consent, children's participation was also voluntary and could opt out. There was a 2-3 weeks' window to fill out the survey. Additional details are included in the appendix 8.3.

3.3.3 Data analysis

This section describes how the data analysis was conducted on the data collected through each method. The results from the analysis are presented in the results chapter.

3.3.3.1 Interviews

The interviews with stakeholders and parents were analysed separately. The stakeholder interviews were not recorded. The key points, observations in the discussion were captured in the form of textual notes during and after the interviews. All the notes and responses were mapped to questions. Interviews with parents were recorded and later transcribed. The transcriptions were mix of verbatim and edited, depending on the conversation (Baxter, Courage and Caine, 2015, p. 252). All interviews were conducted in English, except one which was conducted in Norwegian and later translated. The quotes mentioned in the Results section are direct quotes from the interviews and are not corrected in grammatical and/or sentence structure aspect. To facilitate better understanding, intended meaning and interpretation is added in the square brackets.

All transcriptions and personal data were stored on a secured private server belonging to the AiBA project. Access to this server was limited to the researchers and main supervisor. For the analysis, thematic analysis was conducted on the data. The transcripts were scanned and reviewed for repetitive themes and perspectives. Basic statistics are gathered and analysed to get a better understanding of the data.

Promising re-occurring themes along with some outliers and their interrelations are captured and explained in Results chapter. The thematic analysis was done according to steps outlined by (Nowell *et al.*, 2017). However, the some of steps were modified and updated to suit this thesis. For example, peer debriefing, team meetings and similar steps were omitted. Instead, some of data points and themes were discussed with the supervisor and co-supervisor to get validation.

The interviews also helped get a deeper understanding about the following -

- What scenarios users come across, contextual information of those scenarios
- How their actions differ based on a situation
- Thoughts before and after they have taken the action

3.3.3.2 Surveys

All the collected survey data was anonymous. The raw data was downloaded through Nettskjema and imported into SPSS (version 27.0.1) using codebook export feature of Nettskjema. This exported file readily converts all the questions into variables and options as values when run as script through SPSS. The imported data was cleaned in following ways –

- For consistency purposes, the answer options were arranged in ascending order, i.e. from don't agree to completely agree, frequency responses from never to always etc.
- Variable types were updated wherever required.
- SPSS considered the last option in the question as missing value, which wasn't the case for some of the questions. This was fixed by configuring missing values for each question.

The question that had qualitative answer was not considered in the analysis through SPSS. Once the data cleansing part was completed, following statistical analysis was conducted –

- Frequency analysis was conducted on all the questions and variables.
- Descriptive statistics to understand key features, characteristics
- Independent samples t-test, correlations
- Regression analysis

3.4 Define and Ideate

Traditionally, user centred design projects would visit this phase multiple times in iterations. The focus and time spent in the phase varies according from time to time. And it may be hard to pin point the exact time where it can be said that the phase is officially completed. However, mapping activities to phases helps providing perspectives and understand the process within the context. This phase would focus on understanding data gathered, evaluating whether there are any causal relationships and common themes involved. For this research, defining the key challenges and needs began after going through the raw data and the analysis of it.

After coding and categorizing the raw data, qualitative data was analysed using thematic analysis. Different scenarios and contexts were considered while conducting the data analysis. Key tasks are associated with a scenario or a context can help to have better understanding about what a user can do in the future AiBA app and what interactions could play an important role. These tasks can then be easily translated into a user interface. Alternatively, this phase of the research is also important for confirming assumptions and defining terms which are unknown.

3.4.1 Focus groups

Previously researchers in AiBA have used focus groups and surveys to gather data in same context (Raffel, Bours and Komandur, 2020; Raffel, 2020). Focus group is an established method to gather data and establish context in an informal setting (Stickdorn *et al.*, 2018). The interaction between the participants can flourish multiple ideas and topics that have never been thought about both by participants and researchers (Baxter, Courage and Caine, 2015, p. 340). Focus groups allow researchers to observe participants and it can be done in their natural environment that provides additional information about the surrounding. In this case, conducting a focus group with children at their school would be useful as it is familiar to them. Children often feel comfortable around their teachers and friends at school and thus can participate in the research activities without any apprehension. In total, two focus groups were conducted in this research.

3.4.1.1 Focus group with designers

The first focus group was conducted as a brainstorming session. The participants were students from Interaction Design master's programme. The goal was to generate more ideas on the topic in broader sense the help to solve the research questions. The focus group was planned for 45 minutes, and 4 participants were involved. Participants were required to collaborate using a Miro board (an online collaborative whiteboarding tool), however, the focus group was conducted in-person. There were four activities in total–

- Introduction to the topic
- Activity 1 - How can we increase children's awareness about privacy and grooming?
- Activity 2 - How can we help children to -
    - Cope up with risks/Build risk coping mechanisms
    - Monitor their own actions
    - Collaborate with parents to solve challenges
- Activity 3 - Their feedback on the low fidelity prototype, potential ideas to improve (see figure 11)
- Activity 4 - Voting on ideas and discussion

Miro board was useful in this case, as it helped quickly add sticky notes, text and shapes to the board. All participants can independently work and also see each other's work. Participants were allowed to use Miro to draw ideas on given mockups or use the mockups printed on paper. All the activities had a time limit and did not collect any personal data. More details about the focus group questionnaire can be found in appendix 8.4.

Even though this focus group did not have children as participants, the experiences from it helped to plan out the focus group with children. The time limits for activities and nature of questions could be adjusted to suit children as participants.

3.4.1.2 Focus group with children

The second focus group was conducted with children. The consent to participate in the focus group was obtained in similar ways as that of the survey. The focus group was scheduled for 2 hours, and 9th grade students were invited. The activities were divided in two sessions, with a short break in between.

The first session focused on the following –

- Introduction and ice breakers
- Questions and discussion around online risks
- Understanding their imagination about the future AiBA app, how should it notify and work

The second session consisted of activities based on and around a scenario –

- How can the AiBA app help someone who is facing problems?
- How do children imagine a feature and/or ideas regarding a theme or a context

At the beginning, children were given a quick introduction about how to draw different shapes that can be part of any interface. Children were also assured that anyone can draw with most basic shapes and no drawing is wrong or bad. At the end, there was some time for voting and discussing the ideas. The focus was to keep the group active and get their inputs from activities, discussions. The focus group activities and discussions were facilitated by one researcher while the other took notes on different fronts such as ideas, discussions and overall responses to the questions. Children were rewarded with small treats, candy for their valuable contributions and efforts.

3.5 Prototype

Prototyping as an activity was part of previous phases briefly. Low fidelity (e.g., paper prototypes) prototypes are minor investments which make it easy to change it quickly. Users can relate to something and give specific feedback rather than making assumptions about how it will work (Stickdorn *et al.*, 2018).

These low-fidelity prototypes would then act as a base for co-creation or participatory activity through co-design workshop (Tomitsch *et al.*, 2018) or focus groups, wherein different solution aspects would be tested and captured. Low fidelity prototypes played an important role in getting initial validation from users (both parents and children), and stakeholders. Post the data analysis of all the methods, an improvised prototype is created to summarise all the ideas. It highlights different functionality that can be there in the future AiBA app.

3.6 Testing

Similar to the prototyping phase, the testing phase has been visited briefly while the research and ideation activities were being conducted. The low fidelity prototype was tested with all the stakeholders that are part of the ecosystem. In future, long term effectiveness can be evaluated after a certain time period, to check whether it is increasing awareness and meeting needs that were outlined. The usability testing was conducted in the interviews with parents and stakeholders. Children also provided their feedback on individual features and overall low-fidelity prototype through survey. The discussions and ideas gathered from focus groups are also noted and utilised to create the final prototype.

Following criteria are used to measure the concept(s) –

- Does it protect their privacy?
- Does it solve their challenges?
- Are children willing to use and are they comfortable with such a solution/concept?

Other than usability testing, the dot voting method (Stickdorn *et al.*, 2018) was utilised to reduce the number of ideas generated from the focus group sessions. All the participants were given a time limit to go through different ideas and materials created by other participants. Participants were then voted on top 3 ideas or artefacts. For the focus group with children, the two groups were also asked to vote on one idea among the top ones.

3.7 Ethical considerations

This section highlights ethical considerations when children and sensitive topics are involved in research.

The Norwegian National Research Ethics Committee has published set of guidelines about involving children in research (Backe-Hansen, 2016). The guidelines emphasize that competence and vulnerability of children is highly important when evaluating research projects from ethical aspects. As far as competence and consent is concerned, authors mention that cognitive development of children needs to be considered for participation in research and children’s knowledge has been developing more than thought (Backe-Hansen, 2016). However, according to the author, this needs to be proceeded with caution, as more encouragement on participation in research does not grant children to give consent for themselves and parents or guardians can ask children whether they should give consent on their behalf (Backe-Hansen, 2016). The research considered these guidelines and obtained the consent from both parents and children. Both children’s and parents’ participation was voluntary and it was emphasised.

Backe-Hansen (Backe-Hansen, 2016) advises to weigh harm and benefits of participating in research for children. Most useful approach then is to minimize the discomfort arising out of these questionnaires or interviews, the author explains. It is also advised to give highest importance to a child’s opinion (Backe-Hansen, 2016). In cases where sensitive topics such as grooming are discussed, moral dilemmas or obligations might arise, if a child discloses information that indicates he/she might be at harm (Hansen, NA). In this research, such scenarios were considered and evaluated with supervisors and teachers before the actual research took place.

In another research (Morrow and Richards, 1996), authors suggest to provide clear explanation of the purpose and the researchers’ attempt to obtain informed consent. It further suggests that the researcher needs to be aware that children’s opinion is shaped by multiple factors such as their gender, age, ethnicity and personal characteristics and also the place where research is conducted (Morrow and Richards, 1996). According to (Druin, 2002), a child might have different roles in research, for example as a user, tester, informant or design partner. Based on these roles’ definitions provided in the article (Druin, 2002), this research might put children in the roles of user, tester and informant. However, all roles might co-exist and may not be clearly differentiable when looked at from a general point of view. This overlap between the roles can be caused by questionnaires and methods combined and is beneficial as it increases the contribution and value addition. As mentioned before, to make children comfortable, all the activities with them were conducted in school premises – a familiar, comfortable place with their teachers and friends.

Considering all of these nuances, the activities were planned to adhere to guidelines, while also protecting children’s privacy. The research was conducted only after getting an approval from NSD. Storing and handling of the data is also done according to the guidelines and within the limits of the approval.

4 Results

This chapter elaborates all the results from research activities described in the above sections. After summarising the results, the chapter presents results activity wise – interviews with stakeholders, interviews with parents, survey and focus groups.

4.1 Summary

This section summarises key findings from all the research methods – interviews with parents and stakeholders, survey and focus groups.

Common themes observed in interviews with parents and stakeholders were trust, privacy and communication. Police officers (stakeholders) described that they observe lack of communication between parents and children. Children often hide to avoid embarrassment and might feel that they are the only one feeling or experiencing a particular incident. Most of the times, this lack of communication is the root cause of problems, stakeholders added. Stakeholders also supported children's privacy and acknowledged that privacy needs to be addressed and protected. AiBA stakeholders (decision makers) highlighted that AiBA preserves children's privacy. The AiBA system is something that parents and children understand and use, trusting each other. The purpose is not to sneak in and gather data but to protect children. Parents and stakeholders acknowledged that too many restrictions or limitations are not helpful and is likely to cause friction. However, both groups asserted that there needs to be a way to know what is happening in children's lives.

Communication was strong theme through all the research methods. Although, the results are contradicting. Most parents explained that they communicate with their children periodically on certain occasions. Some parents trust their children that they will approach them in case of an incident. Survey findings show that average rating on "I talk to my parents about conversations I have had over chat apps" is 2.55 (N = 247), wherein 29.4% (N = 78) children strongly disagree. Similar results are observed with 31.3% (N = 83) where children strongly disagreed when asked whether they like discussing their negative online experiences. Moreover, the average scores for questions related to communication with parents are lower than the others.

In total 9 themes were observed in interviews with parents. Trust, monitoring, communication, competence and privacy are major ones out of all themes. To summarise, parents that participated can be ranked on a scale (low, moderate, high). Table 1 depicts the groups and rankings. It was observed that parents that participated fall under two groups with rankings on the scale. For example, parents from group 1 were observed to have moderate competence, whereas the same for group 2 was low. Even though, currently the groups are shown as a combination of certain rankings, it is possible that a larger population will form multiple combinations across themes and groups. For example, a parent can have low competence (group 2) and high trust (group 1). Combination of one or more theme and rankings can form a new dynamic within a parent-child relationship. Figure 12 details a conceptual schema that highlights relationship between all the themes found.

Parents often reflect upon their incidences. Almost all parents had some worries and challenges with being up to date with current technical solutions (competence). Parents and school both communicated to children. Children also were observed to prefer more privacy. Incidents and experiences from different apps also contributed to their understanding of related issues, such as privacy, awareness etc.

It was found that children are in general aware about what data they are sharing with apps and to their friends or followers. Children are also aware about how to keep their data safe and considerable number of children say that they update their apps and check privacy settings.

Table 1 - Ranking parents and themes appeared

Theme	Parent group 1	Parent group 2
Trust	High	Low
Monitoring	Low	High
Communication	High	Moderate
Competence	Moderate	Low
Privacy	Moderate	Low

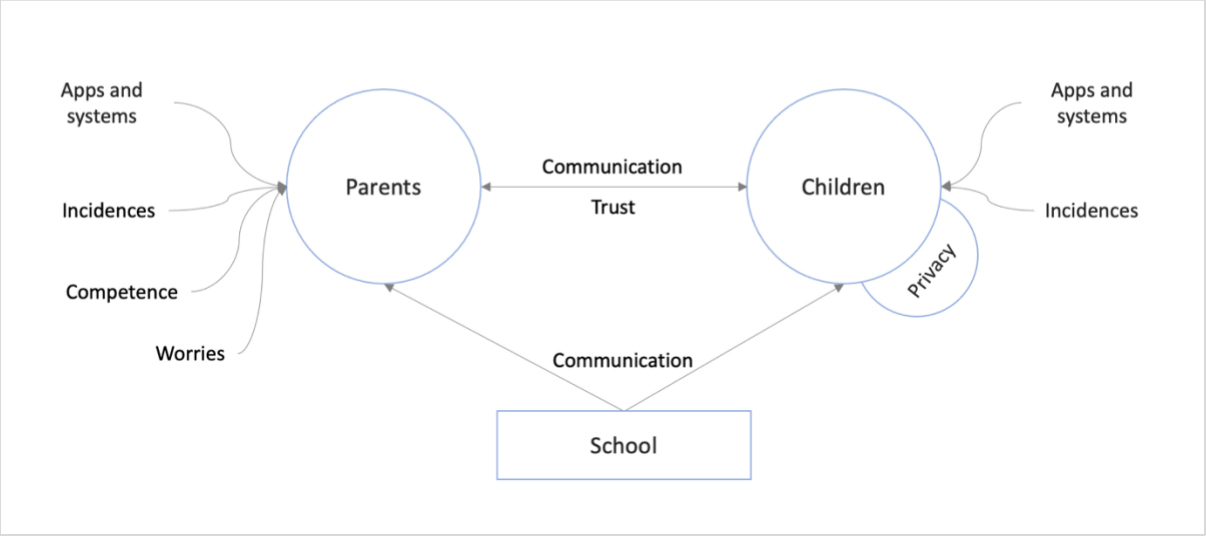


Figure 12 – Conceptual framework to understand relation between themes

Some stakeholders and parents liked the low fidelity prototype (see figure 11) and agreed with some of the content. The primary concerns were around "Remind me later" functionality which might be misused by children to skip this entire task. Moreover, some parents had difficulties to understand the feature "See and change what your parents can see". However, the general consensus was that the solution is likely to help and make children aware.

On the other hand, children favoured features such as "Review your app's privacy settings" was most voted feature with mean value of 3.09 (N=236). Children found the overall solution useful, with mean value of 3.42.

At last, focus group included brainstorming and ideation activities. In the first focus group with designers, broader ideas to solve the challenges were gathered. The participants highlighted different channels or touchpoints where a child and/or a parent can interact. The important feedback gathered was about the content of the low-fidelity prototype. In the focus group with the children, children presented opposing view to parents' opinion that they and children communicate on different occasions. Children did not share details with parents as they thought parents might make a big deal about it and rumours might spread in their circles. In the brainstorming activities, children sketched out the future AiBA app. The most voted sketches i.e., the paper prototypes had common features such as 1) overview of the apps used by a child, 2) monitoring of contacts, 3) warnings when there is potential risk.

As a whole, children welcomed the idea of having such a solution and were eager to work on solving the challenges. The upcoming sections present detailed findings from each of the research methods.

4.2 Stakeholder interviews

Out of the 5 stakeholders that were invited for the interviews, 3 confirmed and participated. The last stakeholder was contacted through a reference of the one previously interviewed stakeholder. Therefore, there were 4 stakeholder interviews that took place. 3 of them were male and one was female. The interviews were scheduled lasted for approximately 40-45 mins with each participant.

Stakeholders were directly and indirectly related to AiBA as a solution. Two of stakeholders, directly related to AiBA were involved in the decision making for development of the solution in both strategic and technical aspects. The roles are AiBA inventor and business developer/project manager. The other two stakeholders were from the Norwegian Police department overlooking different cases in cyber-crime and long-term initiatives that are part of strategic goals for 2025. Specific titles are avoided for the privacy reasons.

The reoccurring and promising themes are explained below.

4.2.1 AiBA ecosystem and future vision

When participants were asked about AiBA solution and their understanding of it within an existing ecosystem of apps, the AiBA stakeholders detailed out how the current solution calculates the risk score that is constantly updated as the conversation between a child and potential groomer progresses. The other stakeholders said that AiBA solution can prevent offensive activities before it goes out of hand. It was also suggested that AiBA is important solution as there are growing number of platforms where children can chat. This was supported by the other police officer –

> *There is a lot of criminal activity and unhealthy usage involved.*

Three stakeholders also pointed out that AiBA plays an important role to help children learn all the risks and protect themselves by giving them a warning to take an action on.

3 out of 4 participants imagined the future AiBA to be an automated system that has better detection and likely to be adapted by multiple industries. The project manager/business developer from AiBA also reported that the AiBA solution has a lot of potential to tackle not only grooming but also mobbing, ghosting, cyber bullying etc. AiBA inventor projected that features such as scanning of images and media shared, are

being explored. This can result into better detection of attempts of grooming. However, stakeholders also mentioned their concern about privacy issues involved getting this feature implemented. In addition, there are challenges in implementing AiBA app that interacts with other chat apps, as the chat apps might use encryption to protect users' data. Upon asking about their imagination of best version the system, the police officer reported that just informing moderators is not sufficient, parents also need to be informed. In case of a potential grooming situation, parents can act quicker than moderators. However, the warning to a moderator is also important as it can allow tracking of a groomer and take necessary legal action, if required.

4.2.2 Trust and involvement in children's lives

All the stakeholders emphasized on trust and communication factor between parents and children. All stakeholders stressed that parents should be involved in their children's lives, in different ways. According to the police officer, most incidences start due to parents not being aware of their children's activities online. These could be prevented much before and comparatively easily, said the police officer citing a murder case involving a child.

As mentioned before in Methods chapter, the interviews were conducted with an assumption about use of parental control/monitoring software. Stakeholders argued against this assumption, describing most parents do not use these apps or solutions. This could be due to regional and/or cultural differences in the ways children are raised. For example, some parents feel that their children can learn through experiences and incidences, and not by listening to parents. Furthermore, another stronger reason is that these solutions could be too technical or too difficult for parents to use. The officer gave an example of YouTube for kids, which was perceived as "not usable". This was due to lack of levels of differentiation in content – as it currently separates content just between adult and not-adult. All the content cannot be segregated using just these two and there have to be more levels. Another example cited was about Snapchat – it does not ask for any authorisation when creating an account or contacting someone. The age restrictions that the platform has, can easily be bypassed.

Further on the issue of using parental control software, AiBA stakeholder supported the learning curve and said –

> *You have to learn [how to use] it [parental control solutions]!*

AiBA inventor supported that there needs to be mutual trust between parents and children. This trust is important for AiBA as an offering to work. The feeling of a system monitoring all the conversations might make it harder to accept. The trust aspect goes hand in hand with privacy aspect. This is elaborated further in the next theme.

4.2.3 Privacy

All stakeholders agreed and supported the importance of children's privacy. Upon asking when parents should start receiving information and how much information should they receive, stakeholders acknowledged that children need their privacy. Privacy aspect is highly nuanced and depends on factors such as parent-child relationship, trust and if parents can/have set up boundaries.

It was observed that there is dichotomy between trust and privacy. More trusting parents are likely to lead to higher privacy for children, however, there are chances of children being exposed to higher risks, if parents don't get to know a risk at the right time. On the other hand, parents wanting to know more details about can lead to lesser privacy, however, potential risks can be mitigated at the right time. It is clear that AiBA maintains privacy and keeps track of just the risk score and the notifications also do not expose any chat content. A stakeholder commented on the privacy aspect –

> *AiBA is not there to sneak into their phones and tell it to their parents. It is there to protect children. It [AiBA] is something parents should tell their children about, if they use it.*

The dichotomy between privacy and trust was resonated by two stakeholders in different ways. The context of the question was, according to the literature review, 89% of parental control or safety apps focus on monitoring aspects (Wisniewski *et al.*, 2017a). Stakeholders maintained that even though children need their privacy, parents are also responsible to protect them. One stakeholder commented,

> *Restrictions can result into friction.*

The stakeholder further explained that there is a fine line between knowing important details and breaching privacy. Just establishing control can also be interpretated as poor communication in a parent-child relationship. Two stakeholders preferred that children are sent a warning about a potentially risky situation and to act on it without getting the warning reaching to parents. Another stakeholder commented in the same context –

> *[Too much] Control always beats trust.*

This partially addresses the issues around privacy and answers some research questions to an extent. The other nuances in privacy are how aware children are about safe practices on the internet and how parents are educating and guiding children.

4.2.4 Feedback on the prototype

The prototype was showed to all the participants and feedback was collected. The collected feedback is distributed in three area groups namely – features, improvements, and general comments.

The overall concept was perceived useful by all stakeholders but one. Interestingly, the exceptional comment was –

> *If I see this as a kid, I will just push "Remind me later". The solution is likely to be discarded as not useful/annoying/not interested.*

The other comments on the overall concept pointed that the solution is general enough to be applied to all the scenarios and can be useful to make children aware about grooming. The stakeholders also suggested that almost all or most of the features could be age specific or targeted towards well defined age groups.

As far as features are concerned, response to "Talk to your parents" and "Scan my messages" was positive. However, one of the suggestions was "Talk to your parents" could be changed to "Talk to someone you trust" as for some children might trust or be comfortable with someone other than their parents. When asked about expectations from "Talk to your parents" two stakeholders said they would expect to see the topics that children and parents can talk to each other about. The reason behind this was to trigger more conversations and provide opportunities where parents can learn as well.

Features such as “Review your messages”, “See and change what your parents can see” and potentially “Review your app’s privacy settings” can be age specific. In addition, the content of the features can be expanded or limited based on a feature and targeted age group. The other improvements based on feature specific age-related restrictions were to have overall restrictive usage for younger children.

One of the AiBA stakeholder highlighted the need to have configurable levels to send or receive warnings. As the future version might have an app, this feature could be available to parents, wherein some of the contacts can be whitelisted or set as trusted. The tolerance for trusted contacts could be higher, for example conversations with close friends.

Overall, the stakeholders were happy about the low fidelity prototype. Moreover, the social media and gaming platforms, can ask for a valid ID when a child (or any other user) tries to create an account. And for children, this can also mean connecting their account(s) to either of their parents’ account and establishing grooming detection system which can warn parents in case of potential risk. One of the stakeholders suggested this as an alternative to the concept. The stakeholder claimed that there are a lot of loopholes or restrictions that can be bypassed to create an account, thus, fake accounts can be created easily. The importance of valid ID and age verification was also stressed.

4.3 Results from interviews with parents

This section describes all the results from interviews with parents. Parents of children from 5th to 9th grade were invited to participate in an interview for 45-60 minutes. In total 16 parents signed up using the sign up form on Nettskjema. 8 parents were interviewed in total, whereas the rest did not respond to consent form and scheduling information.

All the interviews were transcribed and analysed using thematic analysis method. The sub-sections further detail out strong, re-occurring themes that are involved. Microsoft Word was used to highlight and code themes appearing in the transcripts.

4.3.1 Demographical characteristics

Out of 8 parents that participated, 7 were female and 1 was male. The average age of participants was 44 years with youngest one being 36 years old and oldest one at 55 years. Out of 8 parents, 4 parents had two children, 3 had 3 children and one had 5. Considering all these parents’ children, number of boys was more than the number of girls.

One of the questions was targeted to understand parents’ usage of different devices, social media platforms. All but one parents use mobile phones, and computers as their primary devices. For some parents, tablet (mainly iPad) was also part of their day to day lives. Only one parent mentioned use of PlayStation to play games with their children.

When parents were asked for purposes that they use the mentioned devices, key purposes highlighted were work and communication. Other major purposes were to read newspapers, perform banking tasks and use social media and entertainment platforms. Facebook, Instagram, Snapchat and in some cases TikTok were highly used apps among in social media platforms category. Netflix and LinkedIn were other platforms that parents used for entertainment and to be a part of professional communities.

4.3.2 Communication

Communication theme can be looked at from two different point of views – 1) communication between parents and children 2) communication between a school and children.

4.3.2.1 Communication between parents and children

All parents said that they spoke to their children about different topics such as –

- Sensitive or disturbing content that children might see on the internet
- Protecting their personal information by not sharing it with anyone
    - Parents often described and educated their children about pieces of information they should protect. For example, their age, address, real names and so on.
- Not getting involved in a conversation with someone who they do not know
- Avoiding foul or bad language in group chats

Majority of the parents had these conversations on common occasions such as – 1) while the family is having dinner or breakfast, 2) before going to bed, 3) on weekends. Furthermore, separate conversations took place if any incident has taken place, as 3 parents went through problematic incidences that involved foul language and sharing locations to unknown people. One of those incidents was about a child creating an account by different name and taking interest in topics that are not suitable for children. Such events demanded parents to have conversations with their children. One of the quotes from a parent on these lines was –

> *Children do not understand the implications of their actions.*

However, three parents also acknowledged that these conversations might be perceived as boring or repetitive by their children. In addition, while talking about different issues or topics mentioned in the list above, children often replied "I know it already!" or "Of course, we know it!". This highlights the difference in perception about communication between parents and children. Another parent had an opinion that the timing at which this information reaches them is important and as a parent it is likely that they might make a mistake and focus on details that are not important. It is important that children actively remember and practice what their parents tell them to do. One parent found it difficult to have conversations about these topics and expected to have a list handy to take help from.

Looking at communication from children's side, 3 parents described that their children come and talk to them about incidences and content they watch online. The family then could watch it together and discuss.

One of the parents mentioned that they have gotten good amount of information about how to talk to children, however it lacked information about how to protect and what actions to take. When parents were asked about how they talk to their children about safe internet usage, parents observed that children often again respond with "Of course, we know it!" and noticed that they do not bother much about it. However, parents may not know what the real situation(s) is or if there are any risks. One parent's comment regarding this was-

> *I am not going to suspect the kids. I have the impression that everything is fine, but I have no guarantee, or I have no proof.*

When a parent was probed further about communication to make children aware, one concern about moral dilemma in parenting was highlighted. The parent described that their kids have been told not to share real pictures or share any other information. However, that eventually means that they are being told to lie. It becomes a tricky situation wherein parents would want to protect their information and not learn lying to someone, at the same time. The parent comments –

> *When I learn [teach] them to hide and lie, what kind of grownups would they be?*

Another parent wanted to know if a culture-specific content filter would work or not. The parent was concerned about the kind of values are being communicated through these channels and platforms.

4.3.2.2 Communication between a school, children and parents

When parents were asked about information they received from schools, there were mixed and contrasting responses. One parent mentioned that they received information when their child was in 5th grade. However, a drawback was that there was little hands-on training to learn from and it was more of an informative session. There were also some sessions where experts arranged some question and answer sessions. One parent described that schools started to arrange some sessions starting from 2nd grade. On the contrary, another parent mentioned they have not received anything from the school.

One parent highlighted that they needed a way to understand all the risks and did not have any way to explain it to their children apart from talking to them. Another parent commented that there is a need to have content that helps parents and children take concrete actions. The reason behind this was that real-life stories triggers fear and does not help with concrete action. Contrasting opinion was presented by other two parents, in which they described importance of real-life stories to scare children to avoid certain things.

It is likely that children may not talk to parents, if a parent(s) is strict about certain things, one of the parents explained.

4.3.3 Trust

Trust was a one of the strong re-occurring themes and applies to different contexts. Most parents established some ground communication about do's and don'ts on different platforms and it was observed that some did it frequently either naturally or triggered by an event or an incident.

4.3.3.1 Parents' trust on children

Quite a few of parents are part of group chats with their children and other family members on Snapchat, for instance. Three parents mentioned that they follow their children on social media platforms such as TikTok and Snapchat. Two parents mentioned that they do not have access to children's phones or passwords. However, the other two parents mentioned that some parents have access to their children's phones and/or accounts. Herein, parents trust that their children will come and talk to them if they experience anything. As mentioned earlier, one parent quoted in this aspect –

> *I am not going to suspect the kids. I have the impression that everything is fine, but I have no guarantee or no proof.*

Upon probing further, the parent commented that children have not shared any experiences with them. Parents also acknowledged that they could completely be clueless, even if something is happening with children, if they do not share.

One of the parents described that schools encourage them to keep an eye on children's social media, and details such as who do they talk to. And parents do ask about it and receive an answer that everything is okay. While describing this, a parent expressed –

> *I think we have in a way based our relationship on trust, but if the kids want to manipulate [us], then I think they are much better users [of apps/platforms] than we as parents are.*

It was evident that some parents acknowledged that their children could start hiding and do things behind their back, if there is lack of trust. To mitigate this, one parent emphasized on having all the discussions clearly and treating it as natural progression and discuss things as they happen.

4.3.3.2 Children's trust on parents

The trust is rooted in and gets established through some of the regular interactions between parents and children. Couple of parents described that their children talk to them and someone they trust about incidents happened with or around them. The parents also described that the children talk to them if they watch something on the internet. It might be possible that children learn through the lessons from the video and do not need to reveal what happened with them to parents. This highlights that some children are used to having conversations with their parents. This can be termed as children's trust on their parents.

Parents also described that a child need to trust someone, if they are to share some things or if a risk befalls onto them. One of the parents observed their neighbours' children sharing important details of events happening around them. Thus, a child's trusted person could be anyone and they need to be open with them to be able to share.

4.3.4 Monitoring

Parents learn their children's behaviour over a period of time. From the conversations with children, parents get to know through their day-to-day interactions and routines. For example, one parent mentioned that they get to know if someone is ordering something online or playing games and talking to someone. Different levels of monitoring were observed with all parents and changed drastically based on the context.

Children usually complied to some rules, such as not using the internet after 21:00 or not using internet in their rooms. One parent set an expectation that the children need to control and regulate on their own. 4 parents mentioned that they follow their children on the social media platforms and monitor them there. Another parent monitored their children's web searches and page visits to understand if there is anything alarming.

One of the parents highlighted that they could not control or fine-tune the restrictions on the internet for their children, as the existing settings did not fit all their needs. Moreover, the parent felt that they have much less options to monitor their children online. And they do not have required competence to use those options. At certain times, the parent just hopes that everything is okay, and it worries them. This is further complicated if children have internet on their phone (through sim card – mobile data) when they are not at home.

A parent mentioned –

> *I can’t physically go and take their phone and check logs etc. But once they have internet it is not easy to control.*

Another form of monitoring was where parent usually asked their children about their activities online and the content they are watching. This was followed by an occasional reminder about the issues. One of the parents described that, children might fail to read between the lines while they are watching the content online. This might send a wrong message to them (for example, content involving racism, sexism etc.) and can influence their thinking in wrong ways.

There were no gender specific differences in the ways parents monitor their children. One of the parents explained that if they had girls instead of boys, they would have looked at their conversations to see if any pictures are being sent around.

Two parents described having different levels of restrictions and monitoring for their children. The parent described that one of their children was involved in some incidences and felt that the children have different levels of maturities. Age was also a factor to decide when, where and for what purposes a child could use the internet for. For example, even though younger children used the internet, social media platforms, they were allowed to do so only in front of one of their parents. A comment by a parent regarding their daughter’s use of internet was –

> *She hasn’t got the best boundaries in herself, so she needs much more control. And I guess she is less to rely on.*

Most of the parents had control over what games their children can download and play. This was possible as their parents paid for some of the games and still required to approve if there was no payment required. This way parents could be aware about what games their children are playing.

4.3.5 Privacy

Almost all the parents have informed and established that the children are not to share any personal or private information to unknown people. For children that play multiplayer online games, children are also not allowed to talk to strangers i.e., the other players in the game. To avoid the contact, two of the parents that played games had disabled the chat feature(s) in the game. One parent also mentioned that their children were introduced to gaming slowly with other family members so that the children could learn and understand how to behave. In addition, another parent described that their children have to play games in the common area or the living room.

When a parent was asked about, amount of information of they would like to receive from the future AiBA system, the parent preferred to have maximum control and information from it. The parent also believed that the children would agree with it. However, the parent also acknowledged that this might cause a problem for their children’s autonomy. Parents might prefer having maximum control whereas children prefer autonomy.

Interestingly, another parent explained a viewpoint involved in privacy aspect. For this parent, even though they desired more control i.e., want to know all the information and details of children’s usage, they felt that there needs to be some amount of freedom.

The parent says –

> *You really like to have control but at the same time you have to treat your children as they are own person [they are individuals], at least in a way.*

The parent also added that it is necessary to avoid having too many limitations on children's activities and respect boundaries. This might make them do those activities behind parents' back. Two parents also confirmed that they adapt their ways of parenting and monitoring after learning from experiences with their first child.

Two of the parents preferred having more control over protecting privacy in context of risk of grooming. Another two parents wanted the risk notification to be private and only disclosing required information to the parent. Contrasting opinion was presented by a parent that faced some difficulties in some incidences with their child. The parent and the child had had conversations about privacy, however, parents believed that he is too young to think about all these things and thus preferred knowing all the details.

4.3.6 Worries

Some parents are worried over risks that are unknown to them and acknowledged that they have no control over those risks. It was felt this way because it is hard to understand how big a problem is. However, this usually followed by lack of clarity where parents did not know what to do next. A parent commented that –

> *So, I really feel like I have no control.*

Two parents described their concerns about the knowledge they might be lacking. The parents acknowledged that they do not know what they need to know to keep children safe.

A parent mentioned that they are worried that children will come across some age-inappropriate content on the platforms, for example viral suicidal videos on TikTok. Furthermore, the parent explained that children probably do not understand what to do when unknown people contact them, which is worrisome. One parent highlighted specifically their own fears of their children getting contacted by strangers, as the parent was also scared of these things. Regarding the content children watch online, a parent mentioned that they might learn inappropriate details. This can lead to others getting impacted, if a child starts acting on the inappropriate and/or incorrect behaviours. However, a child meeting a stranger of their own age, was not explicitly mentioned or clarified, except by two parents.

It was evident that most of the parent's biggest worry was related to children talking to strangers. One of the parents described this by citing vast nature of the internet and how easy it is to connect to different people. An underlying concern here is that children are likely to come across strangers online and talk to them, either through social media platforms or dating apps and so on. This is worrisome for parents.

4.3.7 Competence

This theme details out how parents observed themselves using all the solutions available at their disposal and how competent they think they are.

Some of the parents felt and mentioned that they do not have that much technical competence to tackle problems related to children's safety online.

Parents observed that technology around them is changing too quickly. 4 parents mentioned that they feel technical aspect is difficult to understand, learn and keep track of. One of the parents described the challenge as –

> *I think, my main concerns are [not knowing] things I don't know. I don't have [technical] skills to use those things. So, I am not able to be aware of everything, I guess.*

The feeling of not knowing everything and not being able to change forced some parents to believe that everything is okay, and their children will come and talk to them in case something goes wrong.

4.3.8 Incidents

One of the other considerable themes was – incidents. Parents described few types of incidents that they experienced with their children or by themselves. One of the parents mentioned that they found some children using bad language in their child's snapchat groups. However, their child was not involved in it. This was followed up by having a conversation with them and checking to see if everything is okay.

All the parents experienced phishing and scamming attempts towards themselves. Two parents also experienced virus attack on their computers, however, they were able to fix it. The degree to which they were affected varied. It also depended on if they experienced it in their workplace or in personal lives. Moreover, most parents experienced these incidences a long time ago. The events were dealt by having stronger passwords and following general recommendations to keep the data safe. The motive of this question was to understand if there are incidences which can be reflected upon, however, these answers about cyber-attacks on parents did not yield stronger insights.

One of the parents observed their child getting a lot of requests from unknown profiles on social media. The parent had been having conversations about this topic and conversations with those strangers did not proceed further.

4.3.9 Feedback on the low-fidelity prototype

When parents were asked about their expectations from the future AiBA app, some of the common responses were –

- The app should be quick and easy to use.
- Parents expected warning from the AiBA app when there is some risk.
- The app should be user friendly. Or should be usable by anyone who is not a technically sound.

Overall, the parents that saw the low-fidelity prototype, liked the solution. One parent felt that this could make their children more aware of the dangers. The parent mentioned a downside of the solution is presenting something that could be too complex for them to understand. The parent described –

> *We are assuming children are more and more mature earlier.*

Amount of time required to invest in this kind of solution was a concern for one parent. As everyone gets exposed to a lot of content and notifications in everyday lives, it is likely to miss these general notifications, until it is really important. In addition, one parent defined good experience is having customizability to suit their family's use.

For one of the parents, it was difficult to understand purpose and usefulness of the feature “See and change what your parents can see”. Building on this feature, the parent described that a child could send a request to hide/show some information and a parent can review it. The app here can advise in favour or against the change requested.

For “Review your app’s privacy” settings, a suggestion was that it can recommend what privacy setting the should children set for their social media platform apps. “Talk to your parents” was perceived to be useful.

In case of “Remind me later”, two parents’ concern was noted that children should not be able to use this more than limited times. Furthermore, if a child skips this check, the chat apps could be locked, and parent can unlock it after a child takes necessary actions.

4.3.10 Miscellaneous

Some parents were part of different socio-political initiatives. These included working for different causes other than their primary area of work or working for different causes as political, social actors. The experiences and observations from these fields were utilised by parents to inform their own knowledge, family dynamics and ways to make children aware. Some parents also cited initiatives by government and social organisations that spread awareness on the topics such as a child’s safety on the internet.

One parent narrated a challenge of children frequently changing usernames in children’s groups on social media platforms. This made it difficult for them to understand which username whose and afterwards they observed an unknown profile in the group. The parent explained that this is highly confusing and risky, even though children might do it just for fun.

One of the parents added a viewpoint about communication from school. The parent was worried about putting most of the responsibilities regarding spreading awareness on schools. The reason behind this was that schools already have many responsibilities, and this would be an additional task to take care of. Key insight from this is that parents also are equal partners in educating and making children aware. On the schools’ part, it is necessary to understand what children need at a specific age and prioritise education in these aspects.

It was observed that responsibilities and tasks that are related to monitoring children, making them aware and such, were shared between parents. For example, one of the participants introduced their child to gaming and chatting in multi-player gaming, whereas the mother asked and monitored their usage of social media platforms. In other parents’ cases, this varied slightly, and parents shared responsibilities such as setting up all the family devices, filtering age-inappropriate content and so on.

A small general observation by couple of parents was that Facebook and Messenger is mostly used by grown-ups these days.

All the parents expected and want to get a warning from a future AiBA system. This warning would mainly to get informed if their child(ren) is talking to someone who is not in their contact list. Another parent expected social media platforms to be equal counterpart towards the entire system. These platforms would be additional channels on which everyone can get relevant information, in addition official channels. A parent desired to have a report functionality, where suspected users will be highlighted with an indication that systems add on their profile.

4.4 Survey Results

This section details out results from survey data analysed using SPSS according to procedure explained in section 3.3.3.

4.4.1 Survey responses and descriptive statistics

As described before, survey was shared with children in two schools from 5th to 9th grade. After two weeks, in total 265 responses were recorded. Out of 265 responses, 262 consented for anonymous voluntary participation and 3 children opted out. Thus, final data analysis considered these 262 responses. The children who answered took approximately 5-15 minutes to complete the survey.

4.4.2 Gender distribution

The survey has almost equal number of responses from boys (N = 123) and girls (N = 133). 6 children chose not to answer the question (see figure 13).

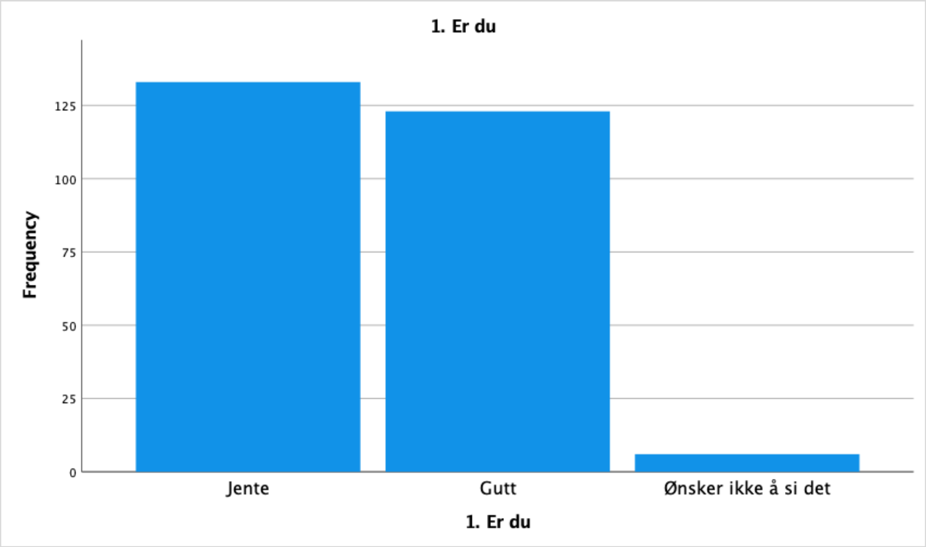


Figure 13 – Gender distribution in survey responses

The survey had very low number of responses from 5th and 6th grade children, 2 (0.8%) responses from each (see figure 14). From 7th, 8th and 9th grade children number of responses were 32 (12.1%), 98 (37.0%) and 126 (47.5%) respectively (see figure 14). 2 (0.8%) children chose not to disclose their grades.

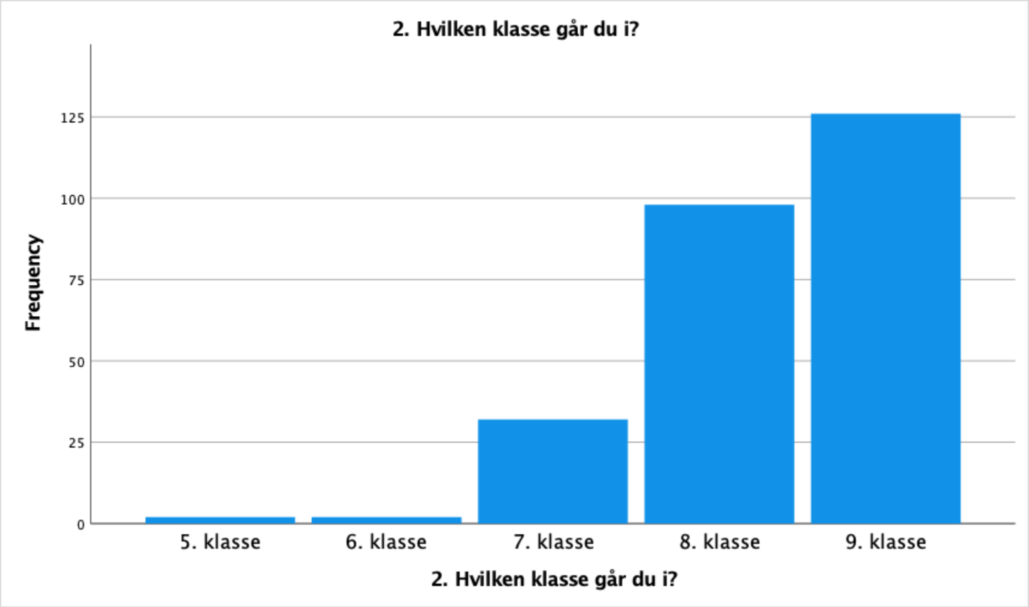


Figure 14 - Responses from grade 5th to 9th

4.4.3 Use of devices and platforms

Smartphone (N = 252, 95.1%), computers (desktop/laptop) (N = 197, 74.3%) and iPads/Nettbrett (N = 162, 61.1%) were most selected options when children were asked about which device they use (see figure 15). Furthermore, considerable number of children (N = 160, 60.4%) also use gaming consoles (PlayStation, Nintendo, Xbox).

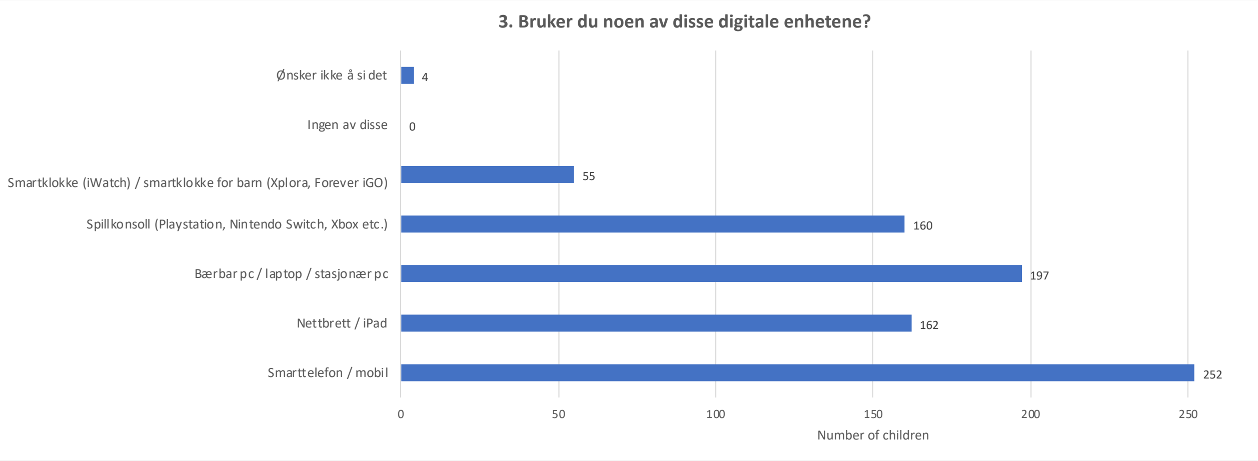


Figure 15 - Use of digital devices by children

When it comes to use of social media platforms, most used apps are TikTok, Snapchat, Instagram and YouTube. Figure 16 shows the usage distribution between apps and time spent on it (highest – more than 2 hours a day, 1-2 hours a day, less than an hour a day, don't use the app or not allowed to use the app). Most children chose that they do not use Messenger for Kids (N=249, 95%) and Telegram (N=248, 94.7%).

TikTok and Snapchat are used for more than two hours by 44.7% (N = 117) and 35.1% (N = 92) of the children. 90 (34.4%) children also spend time on YouTube for more than two hours a day. Children who use TikTok, Snapchat and Instagram for 1 to 2 hours a day are 84 (32.1%), 73 (27.9%), 72 (27.5%) respectively. 76 (29%) children use YouTube for 1 to 2 hours a day 75 (28.6%) children use it for less than an hour a day.

Facebook and Messenger follow similar trends in both more than two hours a day and 1 to 2 hours a day. Children spend less than an hour on Facebook and messenger are 133 (50.8%) and 126 (48.1%). Majority of the respondents for these two platforms are in the "I don't use this app" category and a few spread across the other categories. Facebook received 13 (5%) responses in "I am not allowed to use this app" category whereas the same is 10 (3.8%) for Instagram.

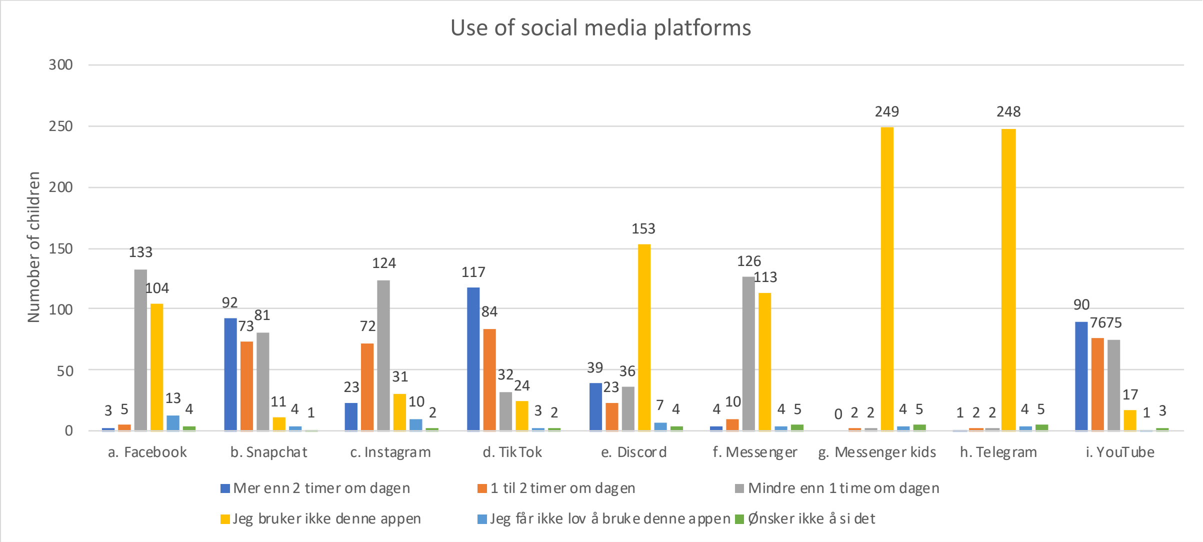


Figure 16 – Use of social media platforms by children

As far as the games are concerned, 21 (8%) and 11 (4.2%) children spend more than two hours a day on Minecraft and Fortnite respectively (see figure 17). Minecraft is played by 34 (13%) children for 1 to 2 hours a day and by 23 (8.8%) children for less than an hour a day. Comparatively more children (N = 60, 22.9%) play Minecraft on weekend or for an hour or two on weekdays. For most of the games, more than 200 children voted "I don't play this game". Effect of this is seen in votes for "Other games" where 76 (29%) children spend more than two hours a day, and 62 (23.7%) children spend 1 to 2 hours a day.

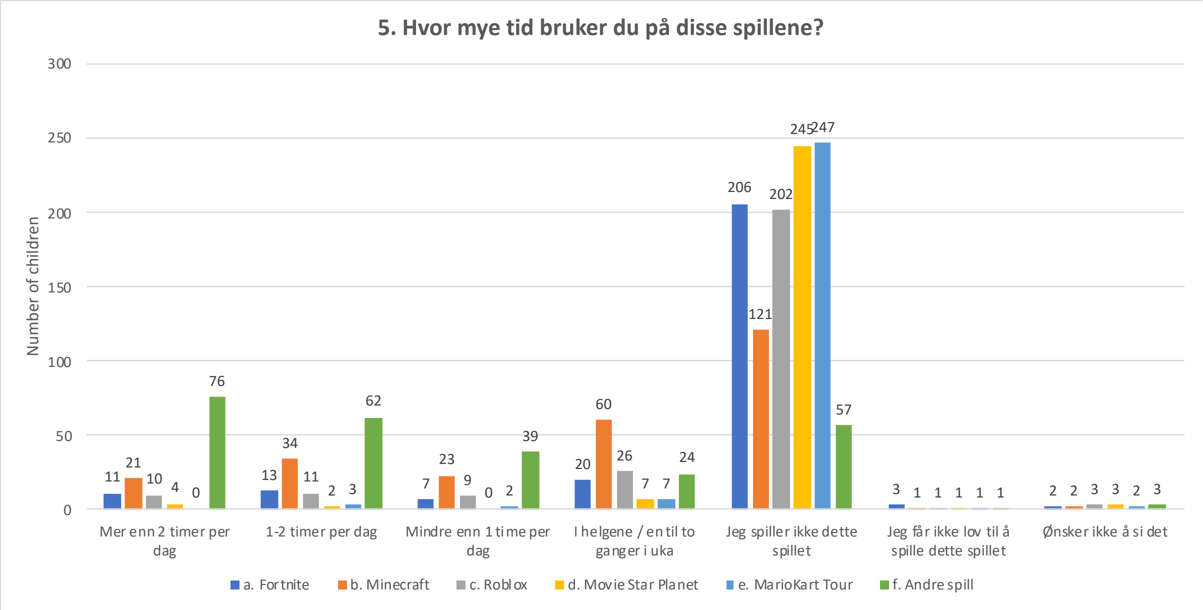
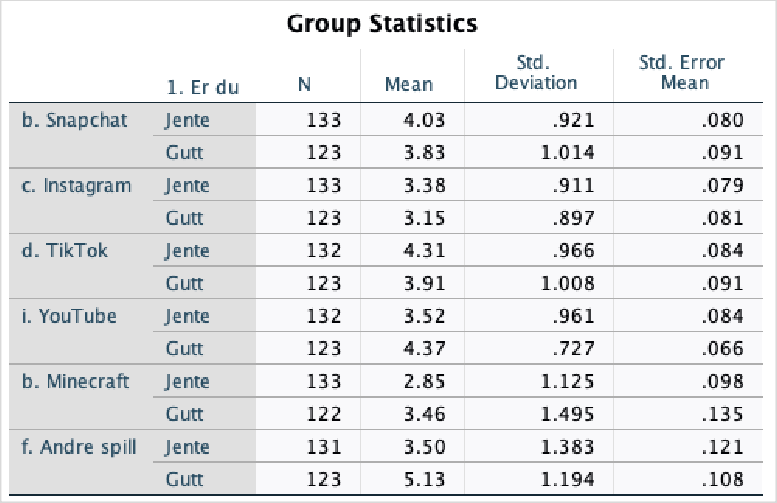


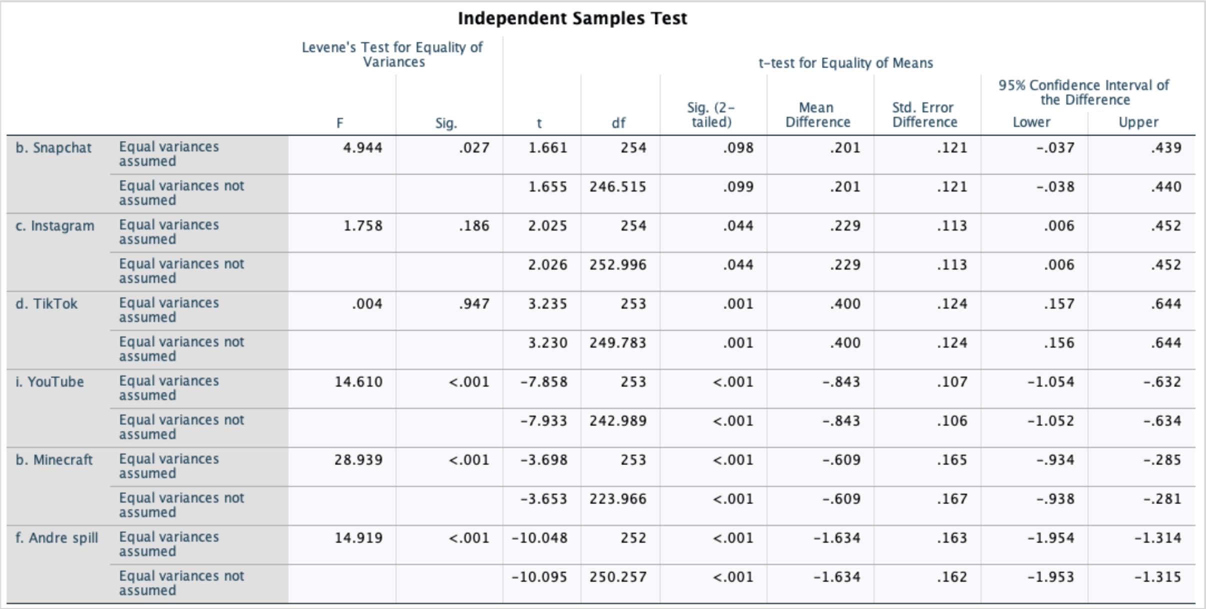
Figure 17 – Amount of time spent on different games

There are gender differences in the way boys and girls use social media platforms and games. An independent samples t-test for top social media platforms (Snapchat, Instagram, TikTok) and Minecraft, other games category are shown in the figure 18.



Group Statistics

	1. Er du	N	Mean	Std. Deviation	Std. Error Mean
b. Snapchat	Jente	133	4.03	.921	.080
	Gutt	123	3.83	1.014	.091
c. Instagram	Jente	133	3.38	.911	.079
	Gutt	123	3.15	.897	.081
d. TikTok	Jente	132	4.31	.966	.084
	Gutt	123	3.91	1.008	.091
i. YouTube	Jente	132	3.52	.961	.084
	Gutt	123	4.37	.727	.066
b. Minecraft	Jente	133	2.85	1.125	.098
	Gutt	122	3.46	1.495	.135
f. Andre spill	Jente	131	3.50	1.383	.121
	Gutt	123	5.13	1.194	.108



Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
b. Snapchat	Equal variances assumed	4.944	.027	1.661	254	.098	.201	.121	-.037	.439
	Equal variances not assumed			1.655	246.515	.099	.201	.121	-.038	.440
c. Instagram	Equal variances assumed	1.758	.186	2.025	254	.044	.229	.113	.006	.452
	Equal variances not assumed			2.026	252.996	.044	.229	.113	.006	.452
d. TikTok	Equal variances assumed	.004	.947	3.235	253	.001	.400	.124	.157	.644
	Equal variances not assumed			3.230	249.783	.001	.400	.124	.156	.644
i. YouTube	Equal variances assumed	14.610	<.001	-7.858	253	<.001	-.843	.107	-1.054	-.632
	Equal variances not assumed			-7.933	242.989	<.001	-.843	.106	-1.052	-.634
b. Minecraft	Equal variances assumed	28.939	<.001	-3.698	253	<.001	-.609	.165	-.934	-.285
	Equal variances not assumed			-3.653	223.966	<.001	-.609	.167	-.938	-.281
f. Andre spill	Equal variances assumed	14.919	<.001	-10.048	252	<.001	-1.634	.163	-1.954	-1.314
	Equal variances not assumed			-10.095	250.257	<.001	-1.634	.162	-1.953	-1.315

Figure 18 – T-test results for usage of social media platforms and games within girls and boys

For Snapchat and Instagram, the gap between mean usage values is smaller. However, it can be observed that for Snapchat, Instagram and TikTok girls use these platforms more than boys. The contrary holds true for YouTube, Minecraft and other games category. The summary of all the t-test results is presented in the table no. 2 below.

Table 2 – T-test results on most used social media platforms and games

App	Results	T-test score
Snapchat	No statistically significant difference	t(246.515) = 1.655, p = 0.99
Instagram	No statistically significant difference	t(254) = 2.025, p = 0.44
TikTok	Statistically significant difference	t(253) = 3.235, p = 0.001
YouTube	Statistically significant difference	t(242.989) = -7.933, p <= 0.001
Minecraft	Statistically significant difference	t(223.966) = -3.653, p <= 0.001
Other games	Statistically significant difference	t(250.257) = -10.095, p <= 0.001

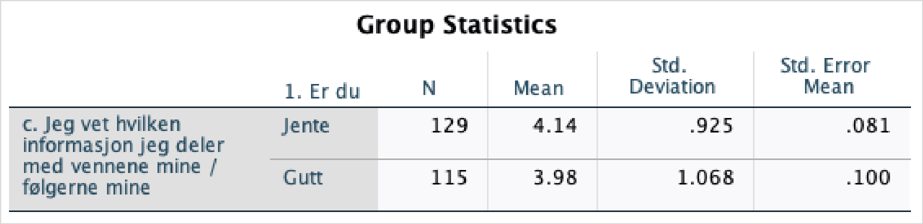
4.4.4 Security and privacy on social media platforms

This section in the survey focused on how frequently children update and check their privacy settings on social media apps. It also asked questions that focused on awareness such as "I know how to keep my data safe" and "I know what data app is gathering about me". In this section's questions, children scored the highest on "I know what information I am sharing with my friends/followers" question, where mean is 4.04 (SD = 1.023). On the other hand, the lowest scored question was "I often check my social media account settings (including privacy settings) regularly", where mean rating is 2.59 (SD = 1.124). The remaining three questions received similar ratings, where mean scores are as follows (see table 3) –

Table 3 – Descriptive statistics on security and privacy on social media platforms

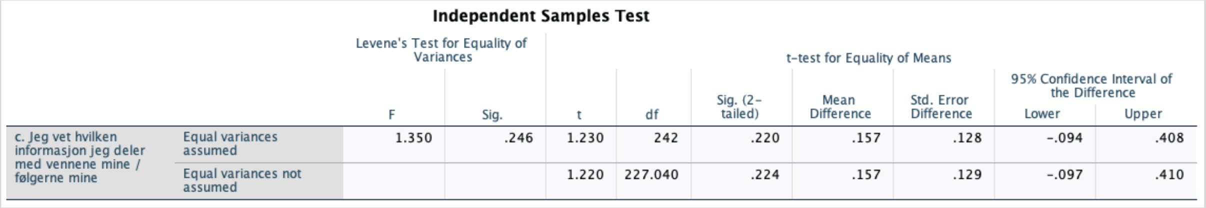
Question	Mean and Standard deviation
I like keeping my apps/software up-to date.	Mean = 3.50, SD = 1.102
I know what information app is gathering about me.	Mean = 3.24, SD = 1.202
I know how to keep my data safe.	Mean = 3.28, SD = 1.243

An independent samples t-test is conducted to understand gender differences in "I know what information I am sharing with my friends and followers". The test results reveal that, girls score more than boys when it comes to knowing what information they are sharing (t(242) = 1.230, p = 0.220). The details are shown figure 19.



Group Statistics

	1. Er du	N	Mean	Std. Deviation	Std. Error Mean
c. Jeg vet hvilken informasjon jeg deler med vennene mine / følgerne mine	Jente	129	4.14	.925	.081
	Gutt	115	3.98	1.068	.100



Independent Samples Test

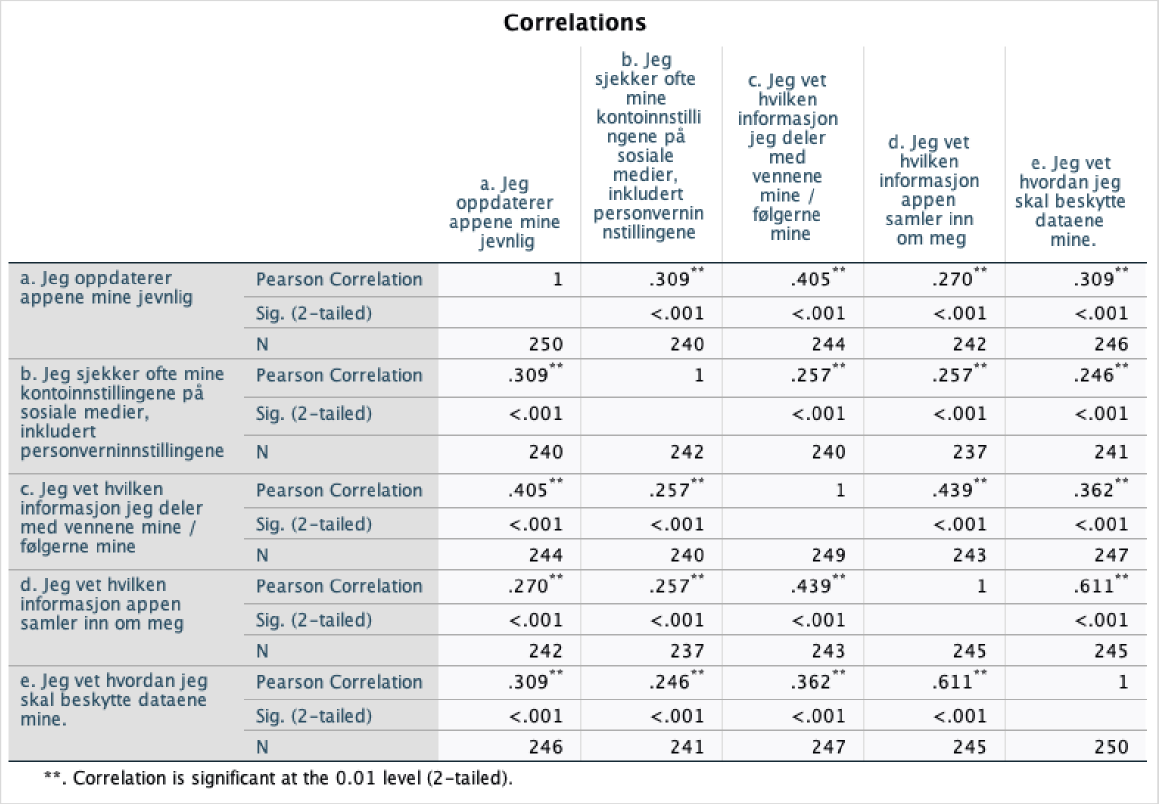
		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
c. Jeg vet hvilken informasjon jeg deler med vennene mine / følgerne mine	Equal variances assumed	1.350	.246	1.230	242	.220	.157	.128	-.094	.408
	Equal variances not assumed			1.220	227.040	.224	.157	.129	-.097	.410

Figure 19 – Independent samples t-test for "I know what information I am sharing to my friends/followers."

There is a comparatively stronger correlation between the following –

- "I know how to keep my data safe" and "I know what information app is gathering about me", where Pearson's correlation coefficient r = 0.611
- "I know what information app is gathering about me" and "I know what information I am sharing with my friends and followers", where r = 0.439

The other correlations are detailed out in figure 20.



Correlations

		a. Jeg oppdaterer appene mine jevnlig	b. Jeg sjekker ofte mine kontoinnstillingene på sosiale medier, inkludert personverninnstillingene	c. Jeg vet hvilken informasjon jeg deler med vennene mine / følgerne mine	d. Jeg vet hvilken informasjon appen samler inn om meg	e. Jeg vet hvordan jeg skal beskytte dataene mine.
a. Jeg oppdaterer appene mine jevnlig	Pearson Correlation	1	.309**	.405**	.270**	.309**
	Sig. (2-tailed)		<.001	<.001	<.001	<.001
	N	250	240	244	242	246
b. Jeg sjekker ofte mine kontoinnstillingene på sosiale medier, inkludert personverninnstillingene	Pearson Correlation	.309**	1	.257**	.257**	.246**
	Sig. (2-tailed)	<.001		<.001	<.001	<.001
	N	240	242	240	237	241
c. Jeg vet hvilken informasjon jeg deler med vennene mine / følgerne mine	Pearson Correlation	.405**	.257**	1	.439**	.362**
	Sig. (2-tailed)	<.001	<.001		<.001	<.001
	N	244	240	249	243	247
d. Jeg vet hvilken informasjon appen samler inn om meg	Pearson Correlation	.270**	.257**	.439**	1	.611**
	Sig. (2-tailed)	<.001	<.001	<.001		<.001
	N	242	237	243	245	245
e. Jeg vet hvordan jeg skal beskytte dataene mine.	Pearson Correlation	.309**	.246**	.362**	.611**	1
	Sig. (2-tailed)	<.001	<.001	<.001	<.001	
	N	246	241	247	245	250

**. Correlation is significant at the 0.01 level (2-tailed).

Figure 20 – Correlations between different factors in the section

4.4.5 Privacy and communication with parents

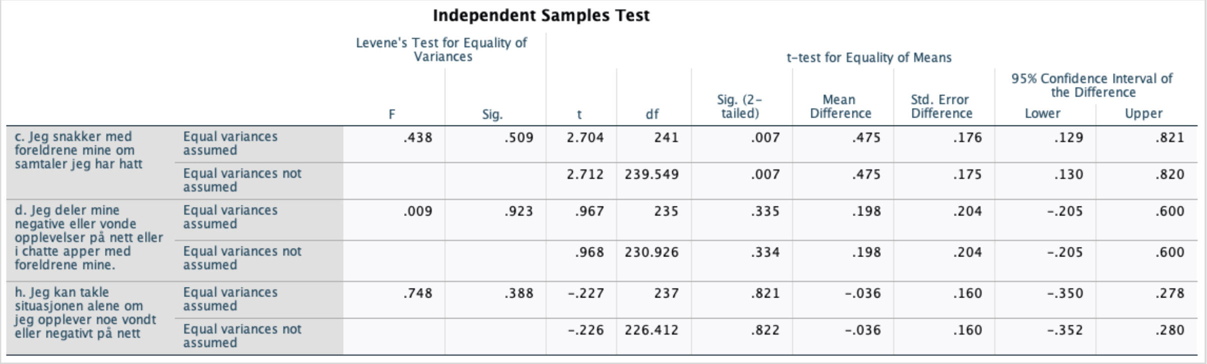
Children rated highest on getting information about risks in usage of chat apps (N = 246, mean = 4.14, SD = 1.195). 30.6% (N = 81) of the children strongly agree that they follow the rules on use of chat apps set up by their parents and 27.5% (N = 73) agree.

On the other hand, average rating on "I talk to my parents about conversations I have had over chat apps" is 2.55 (N = 247), wherein 29.4% (N = 78) children strongly disagree. Furthermore, average ratings on "I like to discuss my negative/strange experiences online (or on chat apps) with my parents" is 2.79 (N = 241) with 31.3% (N = 83) strongly disagree.

89 (33.6%) children strongly agree and 70 (26.4%) agree that they can handle situations after experiencing something concerning on chat apps. 80 (30.2%) children strongly disagree and 45 (17.0%) disagree that they need to talk to their parents after experiencing something strange or negative on chat apps.

Responses in "I talk to my parents about conversations I have had over chat apps" and "I like to discuss my negative/strange experiences online (or on chat apps) with my parents" are correlated with Pearson's Correlation coefficient value r equal to 0.650. Similarly, "I follow the rules my parents have made about using chat apps" and "My parents have told me about risks in using chat apps" are correlated with r value of 0.534.

The result of independent samples t-test between girls and boys in "I talk to my parents about conversations I have had over chat apps" shows that there is a significant difference between boys' and girls' communication with parents (t(241) = 2.704, p = 0.007) (see figure 21).



Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
c. Jeg snakker med foreldrene mine om samtaler jeg har hatt	Equal variances assumed	.438	.509	2.704	241	.007	.475	.176	.129	.821
	Equal variances not assumed			2.712	239.549	.007	.475	.175	.130	.820
d. Jeg deler mine negative eller vonde opplevelser på nett eller i chatte apper med foreldrene mine.	Equal variances assumed	.009	.923	.967	235	.335	.198	.204	-.205	.600
	Equal variances not assumed			.968	230.926	.334	.198	.204	-.205	.600
h. Jeg kan takle situasjonen alene om jeg opplever noe vondt eller negativt på nett	Equal variances assumed	.748	.388	-.227	237	.821	-.036	.160	-.350	.278
	Equal variances not assumed			-.226	226.412	.822	-.036	.160	-.352	.280

Figure 21 – T-test between questions c, d and h

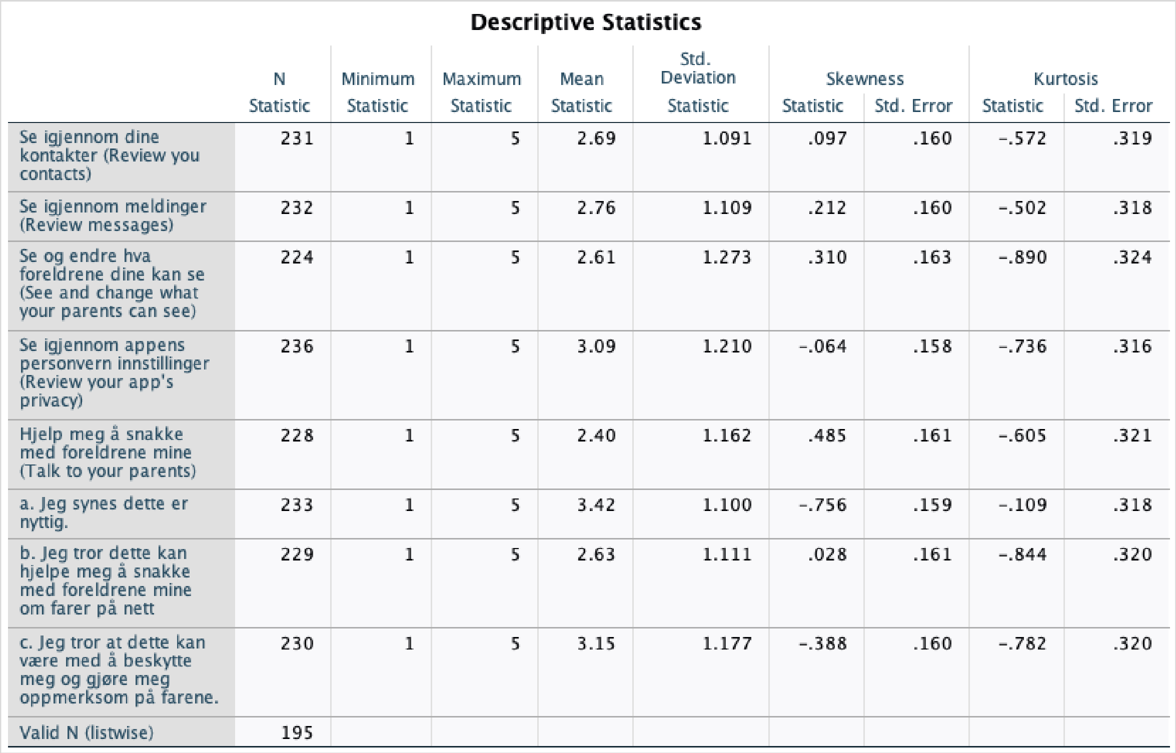
4.4.6 Low-fidelity prototype and overall usefulness

As mentioned before, children were also shown the low fidelity prototype to get ratings on different features. Overall ratings on the usefulness of the solution are also gathered.

"Review your contacts" and "Review messages" have mean ratings of 2.69 (SD = 1.091) and 2.76 (SD = 1.109) respectively. These two features have correlate with Pearson's correlation coefficient r value of 0.715. Features related to communication and sharing data with parents (See and change what your parents can see) has mean ratings of 2.61 (SD = 1.273) and (SD = 2.40) respectively. "Review your app's privacy" has mean score of 3.09 (SD = 1.210).

“Review your app’s privacy” correlates with “Review your contacts” with a r value of 0.545. Both “Review your contacts” and “Review messages” independently correlate with “I find this solution useful” with r value of 0.573 and 0.561 respectively.

On the overall usefulness aspect of the solution, the mean score is 3.42 (SD = 1.10). 109 (41.1%) children agree that the solution (low-fidelity prototype) is useful. On the other hand, 84 (31.7%) children agree that it can protect and make them aware about dangers. The average on “I feel this can protect and make me aware about dangers” is 3.15 (SD = 1.177). Furthermore, the average rating on “I think this will help me to talk about my experiences with my parents” is 2.63 (SD = 1.111), wherein 79 (29.8%) neither agree nor disagree. These are depicted in figure 22.

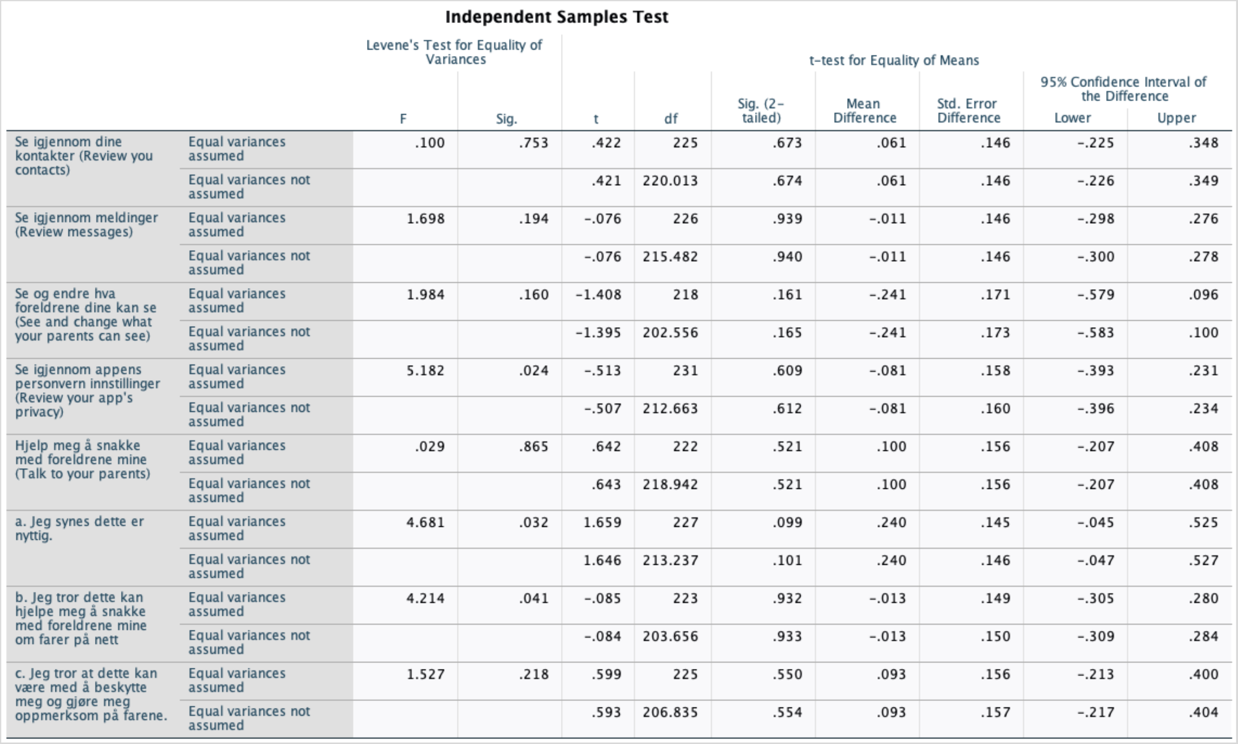


Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation	Skewness		Kurtosis	
	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
Se igjennom dine kontakter (Review you contacts)	231	1	5	2.69	1.091	.097	.160	-.572	.319
Se igjennom meldinger (Review messages)	232	1	5	2.76	1.109	.212	.160	-.502	.318
Se og endre hva foreldrene dine kan se (See and change what your parents can see)	224	1	5	2.61	1.273	.310	.163	-.890	.324
Se igjennom appens personvern innstillinger (Review your app's privacy)	236	1	5	3.09	1.210	-.064	.158	-.736	.316
Hjelp meg å snakke med foreldrene mine (Talk to your parents)	228	1	5	2.40	1.162	.485	.161	-.605	.321
a. Jeg synes dette er nyttig.	233	1	5	3.42	1.100	-.756	.159	-.109	.318
b. Jeg tror dette kan hjelpe meg å snakke med foreldrene mine om farer på nett	229	1	5	2.63	1.111	.028	.161	-.844	.320
c. Jeg tror at dette kan være med å beskytte meg og gjøre meg oppmerksom på farene.	230	1	5	3.15	1.177	-.388	.160	-.782	.320
Valid N (listwise)	195								

Figure 22 – Mean ratings on different features in the low fidelity prototype

A t-test conducted on all the features reveal that there are no statistically significant differences between perceived usefulness of different features and the entire solution (low fidelity prototype) (see figure 23).



Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Se igjennom dine kontakter (Review you contacts)	Equal variances assumed	.100	.753	.422	225	.673	.061	.146	-.225	.348
	Equal variances not assumed			.421	220.013	.674	.061	.146	-.226	.349
Se igjennom meldinger (Review messages)	Equal variances assumed	1.698	.194	-.076	226	.939	-.011	.146	-.298	.276
	Equal variances not assumed			-.076	215.482	.940	-.011	.146	-.300	.278
Se og endre hva foreldrene dine kan se (See and change what your parents can see)	Equal variances assumed	1.984	.160	-1.408	218	.161	-.241	.171	-.579	.096
	Equal variances not assumed			-1.395	202.556	.165	-.241	.173	-.583	.100
Se igjennom appens personvern innstillinger (Review your app's privacy)	Equal variances assumed	5.182	.024	-.513	231	.609	-.081	.158	-.393	.231
	Equal variances not assumed			-.507	212.663	.612	-.081	.160	-.396	.234
Hjelp meg å snakke med foreldrene mine (Talk to your parents)	Equal variances assumed	.029	.865	.642	222	.521	.100	.156	-.207	.408
	Equal variances not assumed			.643	218.942	.521	.100	.156	-.207	.408
a. Jeg synes dette er nyttig.	Equal variances assumed	4.681	.032	1.659	227	.099	.240	.145	-.045	.525
	Equal variances not assumed			1.646	213.237	.101	.240	.146	-.047	.527
b. Jeg tror dette kan hjelpe meg å snakke med foreldrene mine om farer på nett	Equal variances assumed	4.214	.041	-.085	223	.932	-.013	.149	-.305	.280
	Equal variances not assumed			-.084	203.656	.933	-.013	.150	-.309	.284
c. Jeg tror at dette kan være med å beskytte meg og gjøre meg oppmerksom på farene.	Equal variances assumed	1.527	.218	.599	225	.550	.093	.156	-.213	.400
	Equal variances not assumed			.593	206.835	.554	.093	.157	-.217	.404

Figure 23 – Results of t-test for all feature ratings between boys and girls

4.4.7 Role of different factors in solution effectiveness

To understand if factors such as communication with parents and general awareness about good practices on social media apps, a multilinear regression analysis is conducted. The variables calculated and data weighing in into them is depicted in table 4.

Table 4 – Different variables and data weighing in

Variable name	**Data/Questions weighing in**
CommunicationWithParents	- My parents have told me about risks in using chat apps. - I talk to my parents about conversations I have had over chat apps. - I like to discuss my negative/strange experiences online (or on chat apps) with my parents. - I feel the need to talk to my parents, if I come across something strange/negative/unusual. - I find it difficult to talk to my parents about my experiences in chat apps.
Awareness	- I like keeping my apps/software up-to date. - I often check my social media account settings (including privacy settings) regularly. - I know what information I am sharing to my friends/followers/everyone. - I know what information app is gathering about me.

	- I know how to keep my data safe.
FeatureRatings	- Review messages - Review your app's privacy - Review your contacts - Edit what your parents can see - Talk to your parents
InteractionUsefulness	- I find this solution useful. - I think this will help me to talk about my experiences with my parents. - I feel this can protect and make me aware about dangers.

Before performing regression analysis, the data was roughly checked if it satisfies the criteria and does not violate the assumptions. This was done according to guidelines provided by (Berg, No year).

The first regression test considered Awareness and CommunicationWithParents as independent variables and InteractionUsefulness as dependent one. It was found that Awareness (Beta = 0.047, p = 0.341) was not significant factor. Whereas CommunicationWithParents (Beta = 0.271, p = <0.001) was significant. The regression equation is as follows –

$$\text{InteractionUsefulness} = 4.177 + 0.271(\text{CommunicationWithParents})$$

The second regression test considered Awareness and CommunicationWithParents as independent variables and FeatureRatings as dependent one. It was found that Awareness (Beta = 0.204, p = 0.007) and CommunicationWithParents (Beta = 0.212, p = 0.004) were significant factors. The regression equation is as follows –

$$\text{FeatureRatings} = 6.759 + 0.204(\text{Awareness}) + 0.212(\text{CommunicationWithParents})$$

The detailed regression results are added in the appendix 8.6.1.

4.5 Focus group results

As mentioned before, two focus group sessions were conducted. The first focus group was with designers from the interaction design programme.

4.5.1 Focus group with designers

In total, 4 designers (2 males, 2 females) having different backgrounds were invited for the brainstorming and ideation focus group. The session lasted for approximately for an hour. The overall solutions were focused leaned more towards digital side of the solutions. The participants were eager and enthusiastic to participate in the study. They were given a quick introduction to the topic and the research findings that were available at that time.

4.5.1.1 Privacy and children’s awareness

First brainstorming activity focused on the question – “How can we increase children’s awareness about privacy and grooming?”. One of the participants focused on the places the awareness programs or initiatives should engage children on the platforms they interact with the most. In alternative words, it can be said that “meet children on their turf”. In addition, the language of the communication should be informal and easy to understand. Influencers (a term for people with high followers) on social media platforms could contribute to increase children’s awareness about privacy and grooming.

The solution needs to be interactive and share learnings in story telling way to help identify predatory behaviour. Another participant suggested to have a digital diary that children can write in. These incidences can then be discussed with parents. Another version of this in the form of anonymous box of queries or incidences can be installed at school. Based on these, a teacher or visiting expert can talk to children. The social media platforms can also have training exercises to make children aware about privacy.

4.5.1.2 Risk coping mechanisms

Participants wrote broader ideas for helping children build cope up mechanisms. The other two problem areas were – helping children monitor themselves and collaborate with parents.

One of the ideas was to have a government-initiated app that helps parents talk to their children and vice versa. This app or system can also help educate parents through courses on the issues. Parents and children can have easy to remember rules in the form of checklist. The checklist can also be used as a tool to learn about risks they can run into. For example, the rule could be named SNAIL (School Name Address Intimate Location) – it tells all the things children should be careful about when sharing with someone. Here the address is assumed to be a residential address and location is the current whereabouts of a child. This was one of the ideas that received higher votes.

Two participants suggested to have an ability to mark contacts as trusted. The non-trustworthy contacts can have reduced abilities or functionality for example, children cannot share or receive images. The system can also have a message or a pop-up notification that warns children in case they are sharing something to a non-trusted contact. The participant also expected to have stronger, more noticeable ways to report or block a person.

4.5.1.3 Feedback on the low fidelity prototype

One of the activities was to gather feedback on the low fidelity prototype and suggestions to improve it further.

Overall, a participant commented and agreed that the content of the concept feels right. All designers commented on the language part of the concept. The language seemed to be difficult to understand for children. The tone of content can be a little softer.

Designers commented that children could be rewarded when they complete all safety checks. The reward could be a new exclusive sticker pack on Instagram stories, for example. This was one of the most voted feedback items. Instead of having all tasks on one screen, the progression of the tasks could be changed to sequential. Children go through each of them one by one and can see progress bar somewhere on the screen. This feedback received two votes in total.

To summarise, the focus group results focused on broader initiatives that can be taken to help children and parents be more aware. Children can take help from checklists, courses and better reporting/blocking mechanisms. The future solutions need to have stories in the interactive form. In addition, informal tone in the writing is likely to be more effective. Celebrities on different social media platforms can contribute to spreading awareness.

4.5.2 Focus group with children

The second focus group session was planned with some children from Kopperud Skole. In total, 8 children (4 girls and 4 boys) from 9th grade participated in it. All the children were 14 years old, except one who was 15 years old. The children were randomly assigned to two smaller groups with four children in each one. Both groups had girls and boys. The findings from different activities are presented in this section.

4.5.2.1 General observations

Overall, the children were energetic and eager to participate in the focus group activities and also showed curiosity, enthusiasm towards the topics. For the most part, when a question or an activity was presented in front of them, they discussed, debated in that direction. The discussions took place partly in Norwegian and in English. It was observed that some children participated more actively and drove the discussion whereas the rest of the group participated passively and were active intermittently as whole and in their groups. It was fun for them to work with all drawing, sketching and paper materials. Towards the end of the focus group, children's energy levels had gotten low, and difference as compared to the beginning was noticeable. However, they maintained the focus and all the activities were completed in time.

4.5.2.2 Ice breaker sessions

The whole group were asked some ice breaker questions to ease their way into activities. Half of the children had two or more siblings. When children were asked what social media platforms they use daily, the girls and some boys use Snapchat on regular basis. Some of the boys who play games use Discord to talk while gaming and Snapchat otherwise. Some of them also mentioned Facebook Messenger, Instagram and Facetime.

Children were also asked if they had to choose only app to use for the whole week, what would their preference be. Interestingly, seven children chose Snapchat, and one chose Discord.

4.5.2.3 Questions about online risks

When it comes to different devices that children use, some of the children mentioned that they feel safer on a phone than on a computer. Their reasoning behind this was that it is likely to get affected by virus (or malware) attack on a computer than on a phone. Children were also okay with meeting people in real life that they got to know online. One of the girls mentioned that she had met her boyfriend online first. Some children explained that since Gjøvik is a small town it is easier to find out if a person is being dishonest or lying.

Alternatively, some of the boys who played games mentioned that it does not matter if a person(s) that they are playing a game with, is not their age. One of the boys added, if they are rude, they will tell them or block them.

While having these discussions, children debated whether shy people (children) talk more online than in real life. One of the boys acknowledged that their friends or people in they know are likely to be pushier online.

Interesting observations were made when children were asked about what they would do if they found out one of their friends is being treated badly online. A general consensus was that they would talk to their friend and block the person treating them badly. Continuing further, children emphasized that they would not discuss these things with their parents. Similar responses were received when children were asked if they feel like talking to their parents. The reasons behind not sharing were –

- Parents might make a big deal of things happened.
- Children feared that if they told parents, a lot of other people would find out and make it a bigger issue that it actually is.
- One of the children also mentioned that talking to parents might also lead to spreading more rumours about them, if it gets leaked somewhere.

Almost all the children agreed on the reasons above. Some children mentioned that they would talk to their friend(s) in case they face any difficulties.

4.5.2.4 Brainstorming activities and concept ideas

One of the activities that children did was to state their preferences about the future AiBA app. The questions focused on what the app should have and what should it not have or do.

One of the strong and common input was that children preferred having more privacy. Four out of 8 children desired the app to have minimum control on their data and preferred it did not store anything. Children also highlighted that they did not want the app to send or share anything with their parents. One of the children wrote that, children under 12 years can have their parents monitor their activities, whereas children above 12 years can choose whether they want their parents to monitor them. However, complete monitoring of their activities was not desired.

On the app side, the children expect it to be easy to understand, have settings that suit their use and allows configuration. Children also expected to get a notification when there is a risk. When children were briefed about how the AiBA system works, they were amazed and interested in the fact that it can detect grooming and/or fake profiles correctly 98% of the times.

The findings from this activity can be summarised using three keywords – private, user friendly and configurable as shown in the figure 24. The children were also asked to ideate and draw how the AiBA app would look like. This activity was performed individually as well as a group. Children were allowed to discuss while sketching. It was observed that children showed each other their ideas and debated briefly about different parts.

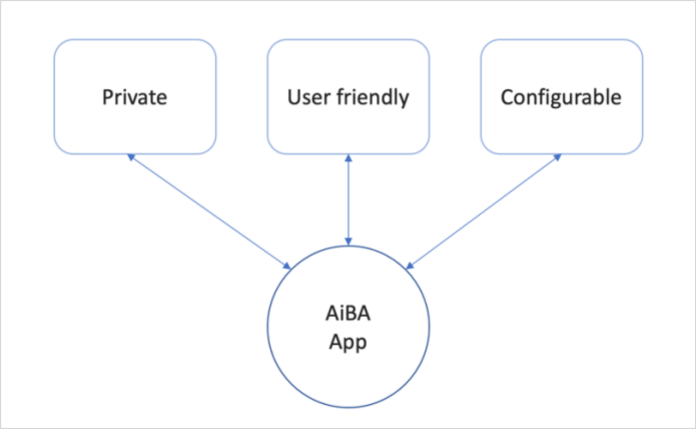


Figure 24 – Keywords that summarize findings from the brainstorming activity

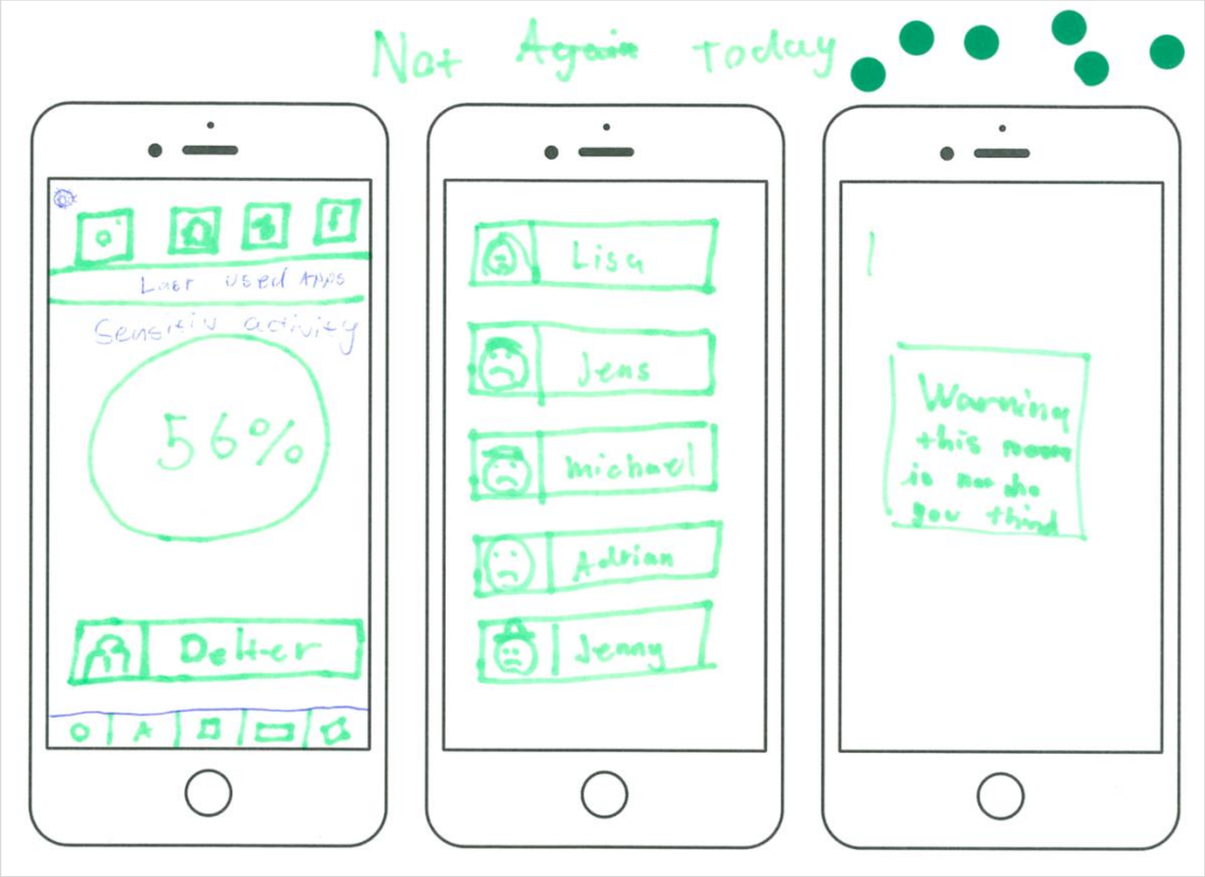


Figure 25 – Most voted AiBA app concept

Children sketched their ideas on paper with phone mock-up printed on it. Most children drew an overview of AiBA app that connected with the other chat apps that would be on their phones. Another common element was overview of contacts that they might be talking to. In addition, some children drew warnings that depicted AiBA app highlighting conversations with potential risk. After the activity, all the ideas were put up on the wall and children voted on their favourite ideas. Each child could vote on maximum of 2 ideas. The ideas that received most votes are shown in figure 25 and 26.

In figure 25, the concept shows all the recent apps used by a child. The system denotes current risk score, or “sensitive activity” determine based on the chats scanned. On the right side, the concept shows contacts that a child is talking to.

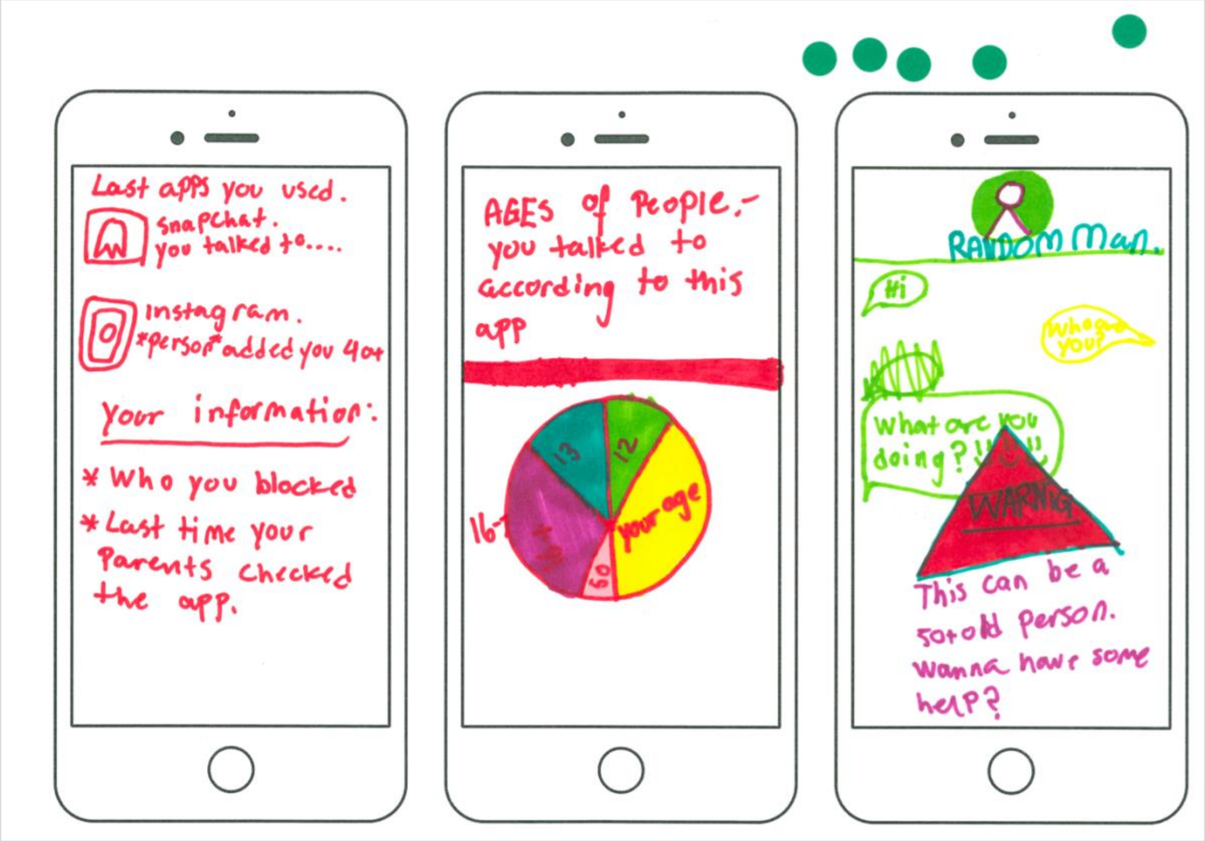


Figure 26 – Second most voted AiBA app concept

In figure 26, the concept also depicts recently used apps and conversations. There is also a section where details such as blocked contacts, when parents checked their usage are shown. Here it is assumed that parents have access to some sections of the app. Interestingly, the concept also shows the predicted age of the people that a child is talking to. When the system detects a risk or suspicion, a warning can be received with an option to receive help.

To summarise, children reflected on their experiences when asked some open-ended questions about their behaviour online. Through the concepts they sketched, common elements were overview of the apps and contacts with warnings for risks.

5 Discussion

This chapter discusses and reflects upon all the results from the research methods. From the literature review, it is evident that some of the older grooming definitions do not apply in perfectly to cybergrooming, however, some overlap is observed between processes from past grooming incidents. The feature review of the children safety apps by (Wisniewski *et al.*, 2017a) observed use of monitoring features as frequently used. Initially, it was assumed that parents monitor children's activities online. However, monitoring through apps or systems was not strongly observed through the research.

As far as the process is concerned, the literature indicate that user centred design methods are used comparatively lesser in the context of this theme. From the results, it is evident that applying the process has some unique contributions and potential to solve the challenges.

5.1 Reflecting on the results

To answer the primary research question – "Can interactions help to induce positive risk aware behaviour that protects children and their privacy?", feedback on the low fidelity prototype and current ways of communicating and monitoring are considered.

Stakeholders highlight that communication, and some amount of monitoring is required to know if there is a risk. It is also important to keep children aware about potential risks that they might come across. Through past incidences the stakeholders observe that currently there is lack of communication and monitoring. Thus, a solution like AiBA is important. The interactions depicted in the low fidelity prototype have good content and can potentially address some of the challenges. However, the prototype stands at a risk of children pushing it away by selecting "Remind me later". Stakeholders also acknowledge that parents lack technical competence to use any complicated safety system for children.

Contrary to stakeholders' opinions, parents acknowledge that they are aware about the potential risks online. It was found that most parents communicate with their children and also trust that their children will come and talk to them in case there is any risk. The parents acknowledged and found the prototype to be useful to make children aware. The parents expected to have a system that sends warnings and provide them information about grooming. Parents also found "See and change what your parent can see" confusing and felt that "Remind me later" could be misused to get away from it. Considering the overall feedback and possible improvements, the solution is likely to be useful to protect and make children more aware.

From the children's point of view, the survey results show that average rating on usefulness of the prototype was 3.42 (N = 233). An arbitrary benchmark for a solution to be accepted and considered is be set to 3. Thus, the concept (and therefore the interaction) can be deemed as useful. Similarly, it can also be said that the children feel that such solution can make them more aware and protect from online risks. The features that were found less useful in the low fidelity prototype need to be re-considered for improvements, for example "Talk to your parents".

Therefore, considering all the angles from stakeholders, parents and children, it can be safely said that interactions depicted above are likely to induce risk-aware behaviour that protects children. This answers the main research question.

5.2 Protecting children’s privacy

Children’s privacy is highly nuanced, contextual and complex in the context of risk. From interviews with parents, it was observed that parents treat privacy differently based on a situation. It is likely that privacy views can change when there is a risk or the tools at hand allow monitoring that can breach children’s privacy. Although, some parents agree children’s privacy needs to be protected.

Children, on the other hand, are consistent in their responses and privacy aspect. In the focus group sessions, children preferred the AiBA app to be private. From the survey results, it is evident that children do not prefer talking to parents about their experiences on chat apps for different reasons. The survey results clarify that some children (17.7% agree, 10.2% strongly agree) talk to their parents about negative experiences and follow the rules set up by them. This can be interpreted in two ways 1) children talk to parents and share all the incidences, 2) children share only details that parents would like to hear and some of the details/incidences are kept to themselves.

Some children expressed that the app could have an option for them to select if parents can monitor them. To understand privacy aspect better, it is important to understand how parents monitor their children. According to the findings, there is a considerable variation between strategies employed to monitor. One of the frequently monitored area is children’s gaming, as it requires parents to pay. In cases where parents have experienced challenges through incidences with their children, monitoring appears to be a bit stricter. While in the rest of the cases, parents trust that their children will talk to them if they are faced with a risk or a challenge. Thus, the assumption that most parents use a children safety app does not hold true. As monitoring in some cases were done through different ways such as having children use the internet in living room or going through their conversations and chats. Parents that trust might lose out on the required communication as there is little monitoring. Children’s age is another important factor of consideration. Younger children might have more restrictions and lesser privacy (doing all the activities in a living room etc.). Whereas the older children may not have such rules and/or restrictions. The age dependent restrictions and interventions are also observed by Wisniewski et al., in their study (Wisniewski *et al.*, 2015). Due to low participation from 5th grade and 6th grade children, the results mostly represent the children from higher grades.

Considering all these details, it can be said that children’s privacy is not compromised in most cases. Children’s use of social media platform and experiences around it, drive the monitoring levels. This in turn can impact the privacy aspect. This answers RQ1 and RQ2 partially. Ultimately, parents can choose to have more details, if they perceive an incident to be serious or critical. Family dynamics are a key factor in protecting children’s privacy. It is likely that this dynamic might change overtime, as children grow older. The rules and communication might continue unless there is a risk or an incident that calls for a change.

5.3 Communication with parents

Communication was one of the key themes involved in the research. Conflicting opinions and results are observed through different research methods.

From the past experiences, stakeholders highlighted the importance of communication, as it can prevent risks causing harm at very early stages. Stakeholders also highlight that a parent needs to be involved in children's internet usage right from the beginning.

On the parents' side, parents are observed to have high and moderate amount of communication with their children. However, the types and details of the communication differ. All parents have had communication regarding safe practices on the internet, for example not disclosing any personal information with strangers, having strong passwords etc. However, some of the parents did not mention discussing the other topics with children such as grooming, privacy. Trust also plays a role in communication, as parents who are trusting, are likely to have less frequent communication with their children. Trusting children blindly or over-trusting can limit parents from seeing potential dangers that children might be in. Thus, it is required for parents to be little cautious or aware of what is happening in children's lives. As one stakeholder pointed out, parents also need to read or get cues from their actions and changes in their behaviour. In addition, if the way parents ask children whether they are facing any issues is the same, children might perceive it as boring and/or repetitive.

On the contrary, this may not be applicable for some their activities on the devices or platforms. For example, parents may observe and monitor activities of children that play games online (on mobile phones or on computers) as parents might have to approve and pay for a game. The frequency of communication varies. It is likely to be more frequent with children that have gone through some incidences in the past, however, it is not measured directly through interviews with parents.

The survey with children brings out the other side of the data. The overall number of children who communicate with parents is less. The data analysis also does not indicate stronger evidence for children wanting a feature that helps them communicate with their parents. This is considered based on the average score for the question "I talk to my parents about conversations I have had over chat apps" which is 2.55 (N = 247). The answers to this question correlates fairly well with the other questions (for example, "I share my negative/strange experiences online with my parents") that investigate parent-child communication. The focus group findings, support these insights. Children expressed their reasons behind not sharing most of the details with their parents. Some children mentioned that they will talk to a friend, when they face any challenges, or their friend(s) faces any challenges.

Thus, it can be said that there is a gap in the communication between parents and children. Similar findings are also reported by Wisniewski et al., who reported relation between parent-child communication and risks (Wisniewski *et al.*, 2017b). The findings can be misinterpreted for that the communication needs to be between parents and children. Although, the communication could happen between a child and anyone he/she trusts and is comfortable to talk to. As one of the parents described that, their neighbour's child often spoke to them to share challenges. Therefore, the future solution needs to redirect the efforts to establish communication towards someone a child trusts. This falls under the Environment part of CREATE action funnel (Wendel, 2014) as mentioned in the background chapter above. Creating a suitable, comfortable environment is important for a desired behaviour and action to take place. In this case, privacy issues are likely to remain the same i.e., likely to be compromised to someone outside a family Eventually, the purpose of having a solid communication with children is not only to understand if they are facing any challenges but also to help them learn risk coping mechanisms, as described by (Wisniewski *et al.*, 2017a). This answers RQ4 up to a certain extent by highlighting current practices.

More restrictions as a result of more communication are counter-productive, even though it may seem as an intuitive and/or logical solution to challenges. As one of the goals is to help them learn and be aware whereas the constraint is not giving too much freedom that can compromise their safety. On the other hand, children might expect more autonomy whereas, parents are likely to desire more control over all the details of risky situations, if not all the conversations. This can likely turn into a conflict situation. Parents are also important part of children's lives and are responsible for their safety and need to be in the loop somewhere.

5.4 Exploring other directions

Regression analysis on the variables – CommunicationWithParents, Awareness, FeatureRatings, InteractionUsefulness, points at some of the population that could benefit from a solution like low fidelity prototype.

For an interaction to be effective or useful, the communication with parents weighs in with a Beta value of 0.271. Thus, children who communicate more with their parents are more likely to use it. However, the awareness does not weigh in significantly. Therefore, children that are aware, are less likely to adopt such solution. At the same time, children that communicate with their parents are likely to use such system and find it useful. From the second regression analysis, Awareness seems to play a role in determining usefulness of a feature. This suggests that a solution's overall usefulness is dependent upon the features that are involved in it, as CommunicationWithParents correlates with Awareness with Pearson's correlation coefficient r value of 0.197.

Based on these two, a theoretical model/framework is proposed (see figure 27). It highlights that predicting effectiveness of a solution in this context is dependent on three different factors – awareness, communication, features involved in it.

There are also other factors that might contribute to determining effectiveness of a solution, for example parents' and children's competence. The reason behind selecting these factors is that these are clearly identifiable and defined areas from the survey design.

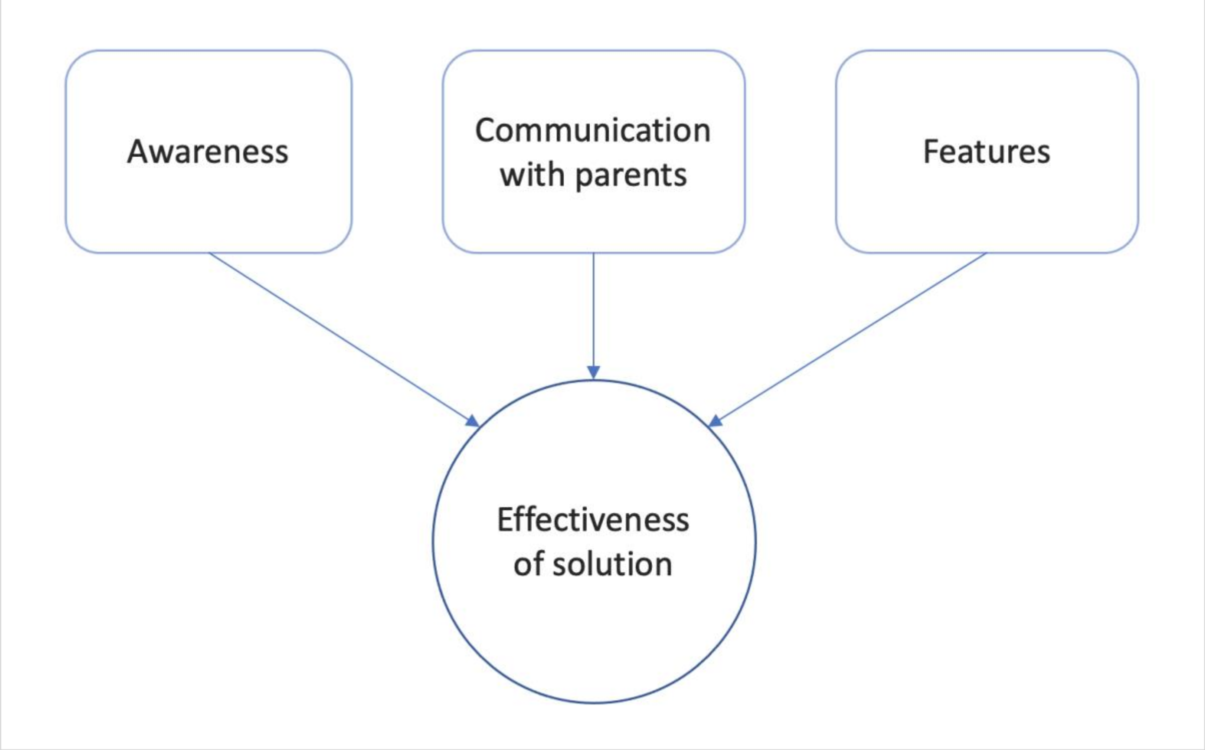


Figure 27 – A theoretical model to determine effectiveness of a solution in context of grooming

5.4.1 Children’s experiences online

The focus group session revealed that children do meet people online. Places where they meet could be online games, through interactions on social media apps. Children also expressed that they meet new people in real life, after meeting online first. These new people who children first meet online, might miss the contextual cues (Kumar *et al.*, 2018) that are present in real life. Thus, the future version of AiBA app needs to consider such interactions that are beyond chat apps.

5.4.2 Gender differences in results

The survey results denote that there are no major differences in behaviours related to different aspects. This is evaluated based on the t-test results in the survey results for use of digital devices and platforms, communication with parents, awareness and ratings on features from the low fidelity prototype. Exceptions to these are use of apps such as TikTok, YouTube, Minecraft and the other games category (see Table 1).

A hypothesis that was based on traditional outlook at the topic was tested to understand gender differences between awareness about the details shared to a child’s followers.

Hypothesis HA– Girls are more aware than boys about what data they are sharing to their followers.

H0 – Girls and boys have similar awareness about what data they are sharing to their followers.

Based on the t-test results, it is evident that there are no statistically significant differences between girls' and boys' awareness about the details they are sharing with their followers and friends. Null hypothesis cannot be rejected. This points out that the girls and boys are somewhat equally aware.

5.4.3 Parents' moral dilemma and dichotomy

It is observed that some parents faced dilemma when they are trying to teach children do's and don'ts to protect themselves on the internet. As described in the interview results, teaching them not to share any real information and asking to lie if someone's asks, might teach them how to lie, in general. This goes against the ideal behaviour expected of children. This might happen knowingly or unknowingly for both parents and children. This might be addressed through more communication and specifying that children have to be conscious about these aspects.

Another example of a conflicting situation is changing usernames. To keep children's identity secure, it is recommended (Raffel, 2020) and they might be told to have a generic username that does not disclose their name or any other personal information. A parent observed that children change their surname frequently. In an online, where a child talks to some of regular friends and some new players, it is hard to identify which username belongs to which child/person. However, chances of this events happening might be lower.

On the other hand, some of the stakeholders mentioned that more control is likely to introduce friction between parents and children. The research suggests, given the parents have required technical competence to use a system, parents might desire maximum control when it comes to risks and children's safety. Based on ease of use of a system (or an app), the future AiBA app can change the way children's activities are monitored currently. As one of the parents pointed out, the time required to monitor and get an overview of children's activities should not be too high.

Differences in communication from schools was observed through interviews with parents. Some parents mentioned that they have gotten information multiple times and from different experts. Some parents did not receive any information. When and how frequently children should receive information needs to be evaluated further. In addition, children might be more influenced or impacted by official sources of information as for many subjects and topics, school is a place where they get introduced to best practices or dos and don'ts. Assuming that children start becoming aware about grooming from 2nd grade, getting information through official channels could play an important role.

To help children understand the implications of their actions, robust detection and warnings are required. For example, if a child is sharing a piece of personal information to a stranger or a new contact, he/she needs to be warned and confirm the action before executing it. Such scenarios can be further built based on communication strategies (Raffel, 2020) outlined by previous researchers working with AiBA.

5.4.4 Parents' competence

Some of the parents reported that they lack the necessary technical skills (competence) to make the most of available technological solutions. Some of the stakeholders and parents also described how the current apps and systems have usability issues in general. To establish stronger communication and understanding about potential risks, parents need learn and adapt to newer technologies and platforms. This also translates to an effort to make the systems more usable and minimize the learning curve. Parents' competence is also consistent with findings and insights given by (Wisniewski *et al.*, 2015).

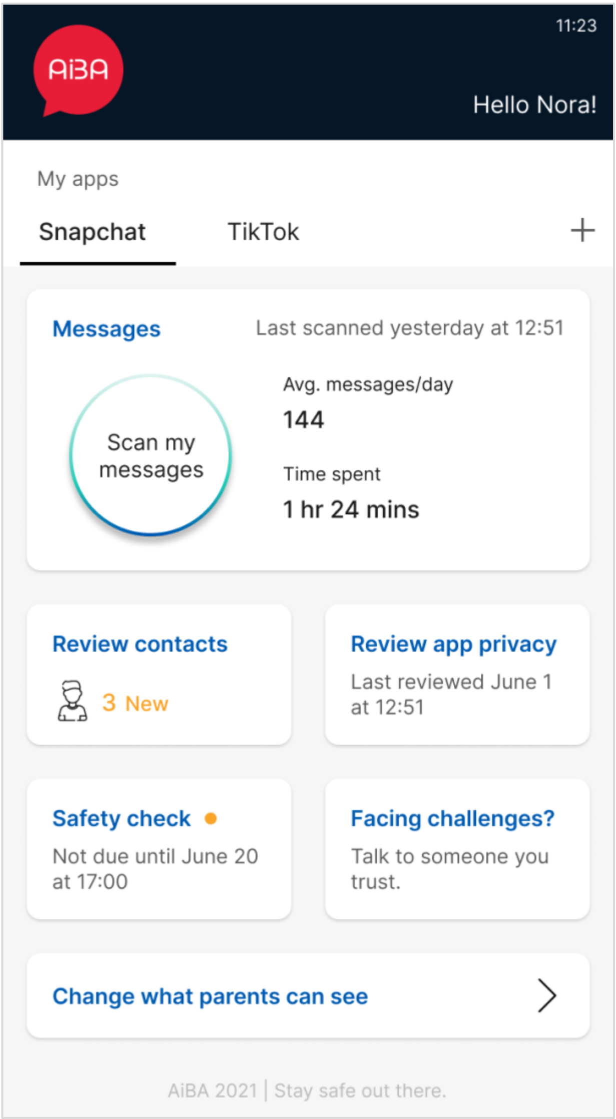
5.5 Improvised prototype

Based on the findings from all the research methods, the prototype is iterated and improvised. The improvements primarily focus on providing an overview of apps that a child uses. The purpose of this prototype is to highlight how some of the key functions of the AiBA can look like, as one of the outputs of this research. It only considers MVA (Minimum Viable Actions) as described by (Wendel, 2014) in the background chapter above. MVA here are the key features and functions that are absolutely crucial to provide the value and utilise the core offerings of AiBA concept. The link to interactive prototype is given in appendix 8.7.

The prototype is created with following assumptions –

- It is assumed that connecting social media apps with the AiBA app is technically feasible. In cases of limited feasibility, it is expected that the scanning and analysis of the chat content is possible through some way.
- The app has all the permissions from a child and parents to access the data on the device. For the app to run and function, all the functionalities that are required are built in and functioning.

After installing the AiBA app, a child needs to sign up using a personal email id in addition to parent's email address. Alternative to email id could be the signing up with one of the social media app credentials that a child uses. A child can connect the AiBA app to all the chat apps on his/her phone.



Messages Last scanned yesterday at 12:51

Scan my messages

Avg. messages/day
144

Time spent
1 hr 24 mins

Review contacts
3 New

Review app privacy
Last reviewed June 1 at 12:51

Safety check ●
Not due until June 20 at 17:00

Facing challenges?
Talk to someone you trust.

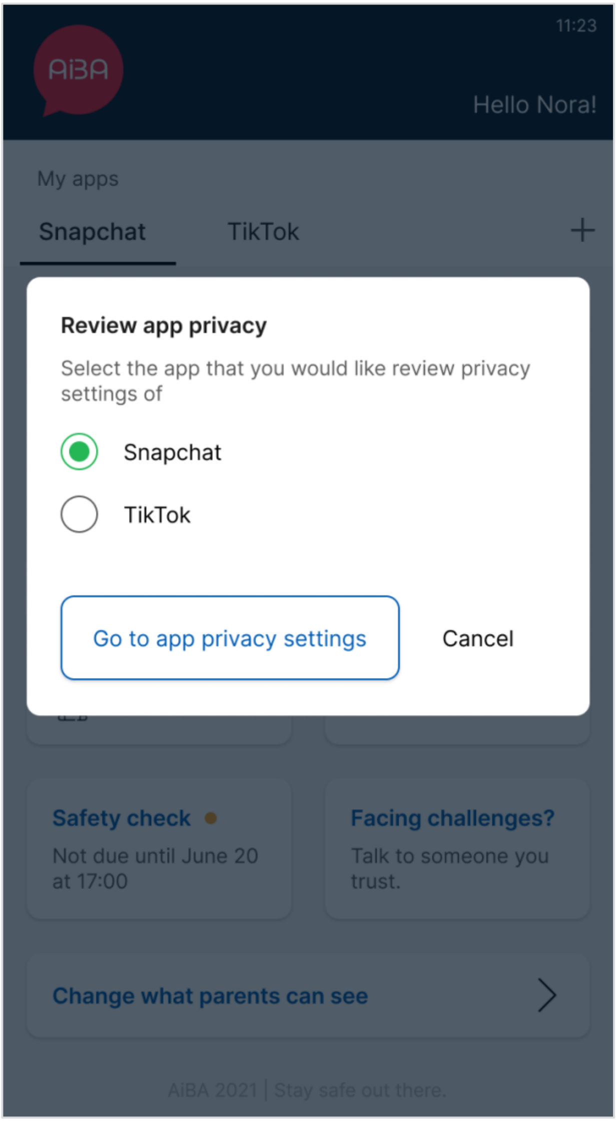
Change what parents can see >

AiBA 2021 | Stay safe out there.

Figure 28 – AiBA app dashboard

On the dashboard (see figure 28), after the launch screen, the AiBA app shows an overview of all the apps with chat functionality connected with the AiBA app. In this case, connected apps are Snapchat and TikTok. Using the + icon in the top corner, more platforms can be added in to the AiBA app. These overviews can be arranged in an order of decreasing usage or apps with decreasing risk. For a given app, a child can see the overview of messages, time spent and scan the messages. The default behaviour is expected to be automatic scanning, detection of grooming risks. However, there might be a scenario may arise wherein automatic scanning may not be possible. Once a child or systems scans messages, a report that highlights different risk and non-risk areas involved within the chats and contacts.

A child can go through contacts that are newly added. These contacts can be set as trusted contacts. A notification can be sent to parents and/or children whenever a new person is talking to a child. Privacy settings of these apps can be reviewed by being in overview of any app. The default selected option will be the app's overview from which the "Review app privacy" is selected (see figure 29).



Review app privacy

Select the app that you would like review privacy settings of

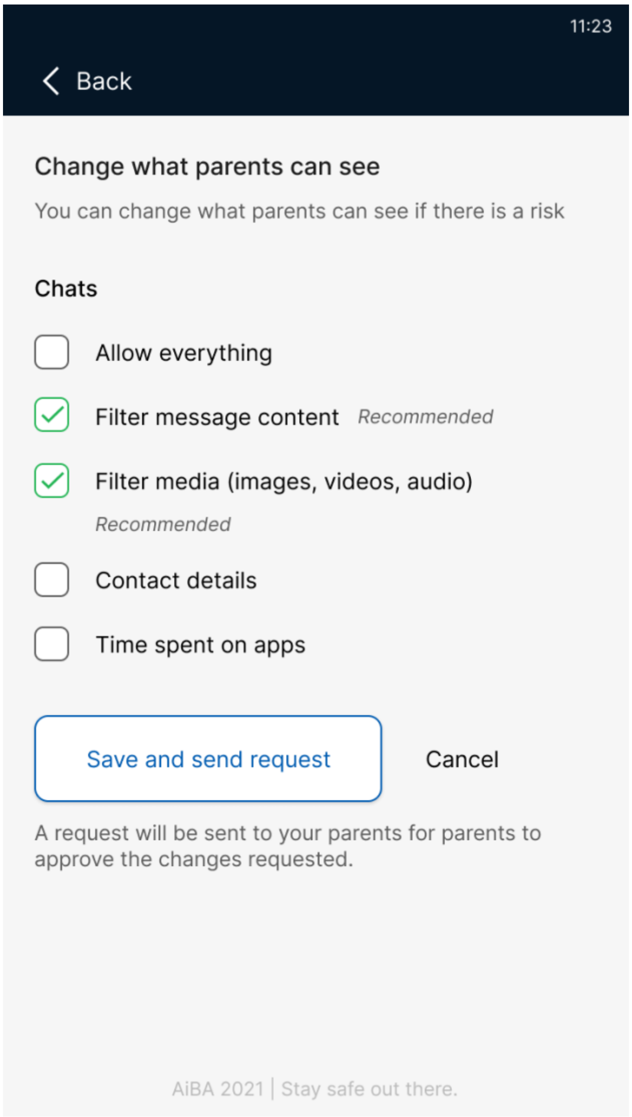
● Snapchat

○ TikTok

11:23
AiBA
Hello Nora!
My apps
Snapchat
TikTok
+
Go to app privacy settings
Cancel
Safety check
Not due until June 20 at 17:00
Facing challenges?
Talk to someone you trust.
Change what parents can see
AiBA 2021 | Stay safe out there.

Figure 29 – Review app privacy

Change and see what parents can see contains all the basic contents that are part of chat apps (see figure 30). The app recommends settings that help protecting children's privacy and is defaulted to filtering messages and content. Whenever a child requests a change in what they can monitor, a parent needs to approve the change.



Change what parents can see

You can change what parents can see if there is a risk

Chats

□ Allow everything

☑ Filter message content *Recommended*

☑ Filter media (images, videos, audio) *Recommended*

□ Contact details

□ Time spent on apps

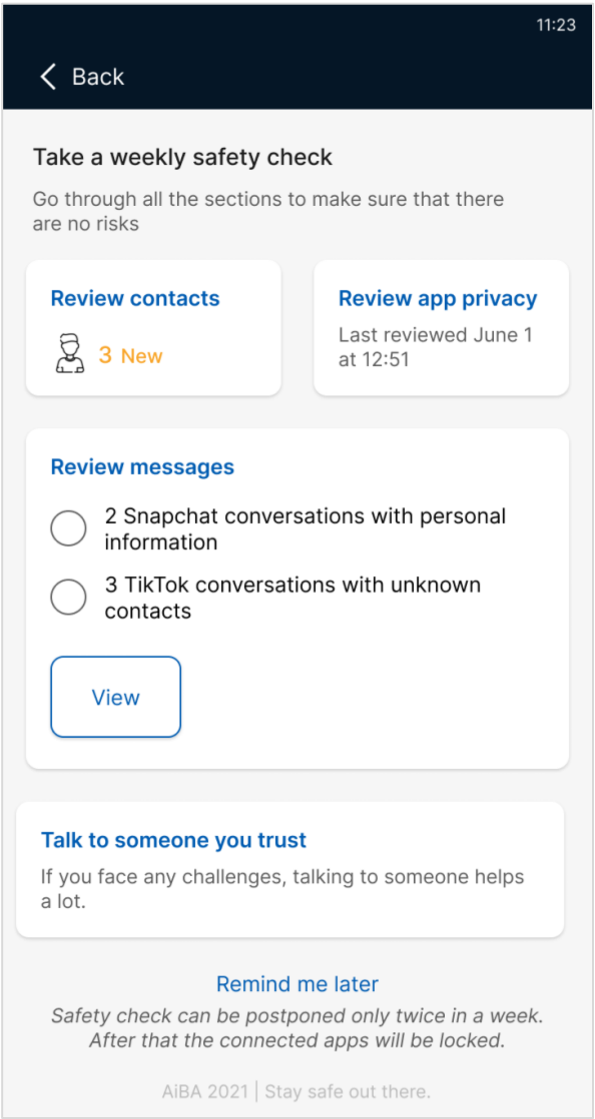
A request will be sent to your parents for parents to approve the changes requested.

AiBA 2021 | Stay safe out there.

Figure 30 – Change what parents see

On the other hand, the weekly safety check (from the low-fidelity prototype) is tweaked to have a review of privacy settings, messages, and contacts (see figure 31). Children can click on remind me later only twice in a week. The next time, a warning can be given to confirm the action and a child can potentially be locked out of the chat app(s). These settings can be present on parents' phone and can be configurable. The time to receive a notification to do a weekly safety check can be configurable. The safety serves the purpose of nudging children in the direction of intended behaviour (Tromp and Hekkert, 2019), as explained earlier in the background chapter.

Overall, this section combined with the earlier background and discussion helps to answer research question number 4 and 5 (RQ4 and RQ5).



Take a weekly safety check

Go through all the sections to make sure that there are no risks

Review contacts

3 New

Review app privacy

Last reviewed June 1 at 12:51

Review messages

○ 2 Snapchat conversations with personal information

○ 3 TikTok conversations with unknown contacts

Talk to someone you trust

If you face any challenges, talking to someone helps a lot.

Remind me later

Safety check can be postponed only twice in a week. After that the connected apps will be locked.

AiBA 2021 | Stay safe out there.

Figure 31 – Weekly safety check

The other potential solution can be to have all these settings and safety check as part of a chat app. However, implications and feasibility of such solution from AiBA and a target chat app is not explored.

5.6 Reflections on methods

The research applied some of the well-known methods from user centred design methodology (Baxter, Courage and Caine, 2015). As explained earlier, interviews helped to gather finer nuances and contexts involved on each side of the problems. There is overlap between the findings from the interviews with the stakeholders and parents.

Interviews with stakeholders brought in unique insights from their experiences working in the field. AiBA stakeholders are key to research to understand the future milestones for the AiBA solution. Police officers are vital as they contributed to reflections and observations from past cases. The semi-structured interviews helped to gather important details as well as probe further in necessary areas. Some of the questions were a bit difficult to understand and answer, due to complex nature.

Beyond getting richer context setting, interviews in general pose a challenge of establishing a specific perspective for a question and obtaining specific answers. This can be solved up to a certain extent by probing further and asking follow-up questions. Some of stakeholders faced challenges to answer questions as their thoughts about children's privacy and when should parents start receiving information. A possible reason behind it could the complex and sensitive nature of the topic. For stakeholders to answer a question, it may be harder to answer a question solely from a stakeholder point of view, as all the stakeholders were also parents. It could be hard to separate these two roles. Thus, it is possible to have their personal experiences to drive their answers. On the other hand, there is small chance that police officers' answers might be biased based on the past experiences.

Similarly, in the interviews with parents, some of the parents faced challenges to understand answer some of the questions. For example, some parents struggled while explaining privacy aspects and their concerns regarding grooming. It is likely that initial briefing and questions might have biased them to answer according to their ideal situations. Parents while answering questions, might idealize their ways of parenting and understanding about these topics, knowingly or unknowingly.

In a study that focuses on qualitative aspects, it is hard to predict effect of different factors on each other. Parents or families might have certain ways to raise children. For example, as one of the parents explained that they miss out on details that need to be told to children. Thus, they talk about things as they happen. In contrast, some might prefer the opposite ways. These differences in raising children are likely to have an impact on multiple factors.

On the practical implementation front, it was challenging to arrange a meeting and setup timing with parents and stakeholders. Scheduling interviews was affected by the global Covid-19 pandemic. As almost everyone had most of their work online, participants are probably hesitant towards having another online discussion or piece of work. In the absence of Covid-19, the discussions could have been arranged in person and can likely get more participants. Having the interviews in person allows researchers to understand the participant better and be empathetic.

While analysing the data from interviews, the outlined themes overlap and are dependent on each other. Furthermore, it is tricky to draw boundaries between them. From a parent's point of view, all these issues such as grooming, bullying, mobbing, privacy etc. could be harder to separate. Thus, a researcher trying to investigate one phenomenon might receive general data that applies to one or more of the problems.

Interviews conducted in this study are prone to instrumentation biases and sampling biases (Leedy and Ormrod, 2015). As mentioned before, the initial questions and briefings might have biased participants to answer in idealistic ways. However, to reduce the biases to minimum the questionnaires were reviewed by supervisors and re-phrased to avoid leading a participant. As far as sampling bias is considered, the triangulation of data from the stakeholders and the parents helps to reduce it up to a certain extent, however, it cannot be completely removed.

On the survey side, the findings helped validate the low fidelity prototype and capture children's communication and awareness details. The surveys inherently bring in response bias. However, as planned before in the course IMT4885 Research Project Planning, the surveys were distributed to more schools and to children from multiple grades to increase participation. This helped to minimise the effect response bias in the survey.

Looking at individual responses, on some of the questions children may under-report or overreport, as they might perceive their own behaviour. For example, children's response towards how much time they spend on different platforms could be under-reported, and social-desirability effect might be at play (Leedy and Ormrod, 2015). A general observation is that people (especially children) are likely to be unaware about how much time they spend on different social media platforms. The same may apply to other questions.

Despite possibility of biases, some of the findings are triangulation of some of the data was possible with the help of focus groups and interviews. This is likely to reduce certain biases and make the study robust.

It was observed that focus groups are a powerful tool to ideate and brainstorm for a given set of problems. It was observed that focus group as a method to conduct research with children is highly effective. Children can participate in activities that are interesting to them. One of the challenges is to plan the right amount of time for an activity, so that children understand, discuss and complete it effectively. Children's attention span also varies for longer sessions or activities. Focus group with designers is also a beneficial method to generate ideas, brainstorm and get feedback on existing ones. It was helpful to have a group that was not involved in the process from the beginning and thus could look at the details from a fresh new perspective. Although it is necessary to have multiple sessions of a focus group, preferably spread over one to three days of different activities. This leaves sufficient time to get participants acquainted with the topic and perform activities in great detail. However, it may be challenging to get a complete day for participants' time at the same time and same place.

Low-fidelity prototypes and/or paper prototypes have been pivotal throughout the process. It played an important role to validate the ideas quickly. The participants can not only imagine the functionality, but also can give better feedback and suggestions for improvements. Paper prototyping is a low cost and low resource tool to quickly get validation and build on each other's' ideas to solve a problem. It was insightful to see children quickly collaborate and combine different ideas by seeing what the other members in their groups have done. The discussions happening around the exchange of these ideas can help establish better understanding of children's usage and thinking.

To summarise, the methods from user centred design methodology are highly beneficial to gather insights to solve children's privacy issues and increase awareness about cyber grooming. Including different stakeholders and children in different parts of the process is necessary and insightful. The methods bring in certain biases, however, the effects of those can be reduced with proper planning and reviews.

The sample involved in the study is highly representative of the population under focus. More details can be understood if different samples are looked at individually. In case of stakeholders, the research considers limited number of stakeholders. With prior experiences within this area, stakeholders can be considered as experts in the field. Parents on the other hand, represent the population partially. All but one of the parents that participated were mothers, thus it can be said that the study is primarily informed by the understanding and opinions of mothers. Fathers can potentially bring in other perspectives or strengthen the existing ones. Looking at higher participation in the survey, the sample is highly representative of the population. Specifically, the findings of the research can be translated to a population with similar characteristics. The characteristics are as follows –

- Mid-size town or city or municipality in Norway
- Children between ages 9 to 15 years, that are part of a mid-size middle school
- Children having access to and using at least one digital device such as mobile, computer/laptop, gaming console and so on.
- Children using social media apps. For example, TikTok, Snapchat, Instagram etc.

Considering all the data, the findings of the research are internally valid. Findings are said to have limited external validity and can be translated with to a population with similar characteristics, alternatively to a bigger population with caution.

5.7 Limitations of the study

The design of the study is kept simple to maximise participation and number of inputs from all the sides. The design of the research has many characteristics of one-shot experimental case study (Leedy and Ormrod, 2015, p. 203). This is likely to inhibit researchers to find and confirm strong cause and effect relationships. In addition, time, scope of the study, and limited availability of the resources are important limitations to be considered.

Due to limited availability of children’s time, a pilot focus group was not conducted with children. Instead, the focus group with designers served both purposes of getting inputs as well as understand what needs to be improved. However, conducting a pilot focus group with children is necessary to validate the questions.

The study considers data from a small time period when the research was conducted. Issues such as privacy, concerns and understanding about grooming are dynamic in nature. Thus, all of these need to be evaluated continuously, possibly with a combination of longitudinal and cross-sectional study (Leedy and Ormrod, 2015, p. 157).

As mentioned earlier, the study precisely targets cyber grooming and privacy and does not focus on other issues that children might face, cyber-bullying for instance. This is important and limiting at the same time as it might be harder for participants to draw a boundary between these issues. This might affect the results and can be harder to retrieve specific information for a given problem.

The study does not test the solution in depth due to time and scope limitations. Although, after initial testing, it is necessary to evaluate the solution continuously in real life scenarios. The real-life usage conditions allow much more scope to evaluate all the interactions and measure specific criteria in greater details.

At last being limited to evaluating interactions, communication and awareness, the study lacks deeper focus into challenges faced by children while using chat app or functionality in different platforms. The issues need to be evaluated in specific contexts and platforms.

6 Conclusion and future work

Day by day the number of children using chat apps and other digital platforms is on the rise. Larger part of everyone’s lives is spent on digital platforms and newer platforms are entering the market. The global pandemic Covid-19 has made this difference even stronger, leading to a completely digital life. The motivation behind this research was to understand how interactions can contribute to induce risk-aware behaviours in children. A lot has been explored and studied when it comes to grooming, theories and processes behind it. This groundwork offered a solid foundation to build research on.

Many examples around us indicate that our interactions with technology changes and impact many aspects of real lives. Interaction design and user centred design have been valuable methodologies that contributed to gather the aforementioned insights and findings. Since the methods are put the human aspect at the centre of everything, true potential of interviews and focus groups was experienced in understanding finer nuances, dynamic relationships between parents and children. The study contributes to increase the utilisation of user centred design methods as those are less explored in areas relating to child safety.

The research answers how the interactions can be effective to make children aware and build risk coping behaviour. Trust, privacy, communication and monitoring are key themes that appeared in the data. On the children’s side, the interactions are effective and are perceived useful. However, it needs to be tested in real life scenarios and usage conditions. Children are aware about the data they share with their friends and followers. Children perceive that they are able to protect their information and handle risks by themselves. These findings are applicable to similar contexts and population with similar characteristics.

Collaborating with AiBA project and conducting the research as a part of it has been highly beneficial. The solution being technically strong is reassuring, the participants could imagine, reflect and focus on the other aspects of the solution. Given the dynamic nature of the problems, the output from this research is a helpful guide for taking critical decisions about the future AiBA solution. It also highlights potential future directions that a researcher working with AiBA can take.

6.1 Future work

A fully functional prototype can be researched and developed. Further, these iterations can be tested in real life environment and with both parents and children. The prototype can be co-created with participation from stakeholders, parents and children. Co-creating together has a lot of potential to discover newer insights and solutions. This enables a researcher to understand how parents’ and children’s interactions with the solution differ over a period of time. The existing frameworks and theoretical models can be tested and improvised to form better alternatives.

Separate efforts can be redirected towards discovering new strategies to establish children’s communication with someone they trust. To understand stronger, cause and effect relationships, different experimental designs such as true experimental designs (Leedy and Ormrod, 2015, p. 204) can be utilised.

Similarly, school teachers' contribution can be higher. School teachers can help to explore newer directions and validate the existing ones. This research acts as a good starting point and opens up a number of possibilities to explore new directions as follows –

- Future researchers can also evaluate and review materials that utilised to communicate risks to children.
- The work can be replicated in larger cities and potentially in other countries or in low populated areas. Comparing and contrasting the results can help make the AiBA offerings robust.
- The role and influence of cultures on a children's safety and privacy can be explored and understood.
- Performance of such system can be tested in two or more age groups of children and parents.
- Parents, teachers and children can team up and co-create design solutions based on key themes identified in this research

It is believed that this thesis lays down all the necessary groundwork to enable future researchers to perform further research and also provides valuable insights to audience.

7 References

ACM (2021) ACM digital library. New York: Association for Computing Machinery.

Aranda, J., Ali-Hasan, N. and Baig, S. (2016) *I'm just trying to survive: an ethnographic look at mobile notifications and attention management*. Unpublished paper presented at Proceedings of the 18th International Conference on Human-Computer Interaction with Mobile Devices and Services Adjunct. Florence, Italy.

Backe-Hansen, E. (2016) *Children*. Available at: https://www.forskningsetikk.no/en/resources/the-research-ethics-library/research-on-particular-groups/barn/ (Accessed: 14 Dec 2020 2020).

Badillo-Urquiola, K. *et al.* (2019) *Stranger Danger! Social Media App Features Co-designed with Children to Keep Them Safe Online*. Unpublished paper presented at Proceedings of the 18th ACM International Conference on Interaction Design and Children. Boise, ID, USA.

Baxter, K., Courage, C. and Caine, K. (2015) *Understanding your users : a practical guide to user research methods*. Morgan Kaufmann.

Berg, R. G. v. d. (No year) *SPSS Multiple Linear Regression Example*. Available at: https://www.spss-tutorials.com/spss-multiple-linear-regression-example/#data-checks-and-descriptive-statistics (Accessed: 28 May 2021).

Black, P. J. *et al.* (2015) A linguistic analysis of grooming strategies of online child sex offenders: Implications for our understanding of predatory sexual behavior in an increasingly computer-mediated world, *Child Abuse Negl*, 44, pp. 140-149. doi: 10.1016/j.chiabu.2014.12.004.

Cale, J. *et al.* (2021) Crime commission processes in child sexual abuse material production and distribution: A systematic review, *Trends & Issues in Crime & Criminal Justice*, (617).

Craven, S., Brown, S. and Gilchrist, E. (2006) Sexual grooming of children: Review of literature and theoretical considerations, *The journal of sexual aggression*, 12(3), pp. 287-299. doi: 10.1080/13552600601069414.

Dam, R. F. and Teo, Y. S. (2020) *5 Stages in the Design Thinking Process*. Available at: https://www.interaction-design.org/literature/article/5-stages-in-the-design-thinking-process (2020).

Dingler, T. and Pielot, M. (2015) *I'll be there for you: Quantifying Attentiveness towards Mobile Messaging*. Unpublished paper presented at Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services. Copenhagen, Denmark.

Druin, A. (2002) The role of children in the design of new technology, *Behaviour & Information Technology*, 21(1), pp. 1-25. doi: 10.1080/01449290110108659.

Emmel, N. *et al.* (2017) Accessing Socially Excluded People — Trust and the Gatekeeper in the Researcher-Participant Relationship, *Sociological research online*, 12(2), pp. 43-55. doi: 10.5153/sro.1512.

Fogg, B. (2009) *A behavior model for persuasive design*. Unpublished paper presented at Proceedings of the 4th International Conference on Persuasive Technology. Claremont, California, USA.

Fogg, B. J. (2002) Persuasive technology: using computers to change what we think and do, *Ubiquity*, 2002(December), pp. 2. doi: 10.1145/764008.763957.

Gillespie, A. A. (2002) Child protection on the internet-challenges for criminal law, *Child & Fam. LQ*, 14, pp. 411.

Gray, C. M. *et al.* (2018) *The Dark (Patterns) Side of UX Design*. Unpublished paper presented at Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. Montreal QC, Canada.

Gray, D., Brown, S. and Macanufo, J. (2010) *Gamestorming : a playbook for innovators, rulebreakers, and changemakers*. Bejing: O'Reilly.

Gunawan, F. E. *et al.* (2016) Detecting online child grooming conversation, *2016 11th International Conference on Knowledge, Information and Creativity Support Systems (KICSS), 10-12 Nov. 2016*. pp. 1-6.

Hansen, A. S. (NA) Co-Design with Children - How to best communicate with and encourage children during a design process. Available at: https://www.ntnu.edu/documents/139799/1279149990/13+Article+Final_anjash_fors%C3%B8k_2017-12-07-20-11-11_Co-Design+with+Children+-+Final.pdf/b8dd19c4-d2b1-4322-a042-718e06663e13 (Accessed: 14 Dec 2020).

Kimmel, A. J. (1996) *Ethical issues in behavioral research: A survey*. Malden: Blackwell Publishing.

Kumar, P. *et al.* (2018) *Co-designing online privacy-related games and stories with children*. Unpublished paper presented at Proceedings of the 17th ACM Conference on Interaction Design and Children. Trondheim, Norway.

Laffey, K. (2020) *How to see your message requests on Instagram, accept or ignore a message, or block a user*. Available at: https://www.businessinsider.com/how-to-see-message-requests-on-instagram?r=US&IR=T (Accessed: 12 April 2021 2021).

Lanning, K. (2018) The Evolution of Grooming: Concept and Term, *J Interpers Violence*, 33(1), pp. 5-16. doi: 10.1177/0886260517742046.

Lanning, K. V. (2005) Compliant child victims: Confronting an uncomfortable reality, *Viewing child pornography on the internet*, pp. 49-60.

Leedy, P. D. and Ormrod, J. E. (2015) *Practical research : planning and design*. 11th ed. edn. Boston: Pearson.

Livingstone, S. and Smith, P. K. (2014) Annual research review: Harms experienced by child users of online and mobile technologies: The nature, prevalence and management of sexual and aggressive risks in the digital age, *Journal of child psychology and psychiatry*, 55(6), pp. 635-654.

Lockton, D., Harrison, D. and Stanton, N. A. (2010) The Design with Intent Method: A design tool for influencing user behaviour, *Appl Ergon*, 41(3), pp. 382-392. doi: 10.1016/j.apergo.2009.09.001.

Meyer, M. (2015) *Machine learning to detect online grooming*, Uppsala universitet, Institutionen för informationsteknologi.

Mladenović, M., Ošmjanski, V. and Stanković, S. V. (2021) Cyber-aggression, Cyberbullying, and Cyber-grooming: A Survey and Research Challenges, *ACM Comput. Surv.*, 54(1), pp. Article 1. doi: 10.1145/3424246.

Morrow, V. and Richards, M. (1996) The Ethics of Social Research with Children: An Overview, *Children & society*, 10(2), pp. 90-105. doi: 10.1002/(SICI)1099-0860(199606)10:2<90::AID-CHI14>3.0.CO2-Z.

Nowell, L. S. *et al.* (2017) Thematic Analysis: Striving to Meet the Trustworthiness Criteria, *International journal of qualitative methods*, 16(1), pp. 160940691773384. doi: 10.1177/1609406917733847.

NTNU (No year) *AiBA (Author input Behavior Analysis)*. Available at: https://aiba.ai/ (Accessed: 1 Dec 2020 2020).

Ou, L. C. *et al.* (2004a) A study of colour emotion and colour preference. Part II: Colour emotions for two-colour combinations, *Color Research & Application*, 29(4), pp. 292-298. doi: 10.1002/col.20024.

Ou, L. C. *et al.* (2004b) A study of colour emotion and colour preference. Part I: Colour emotions for single colours, *Color Research & Application*, 29(3), pp. 232-240. doi: 10.1002/col.20010.

Pielot, M. *et al.* (2014) *Didn't you see my message? predicting attentiveness to mobile instant messages*. Unpublished paper presented at Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. Toronto, Ontario, Canada.

Pielot, M., Vradi, A. and Park, S. (2018) *Dismissed! a detailed exploration of how mobile phone users handle push notifications*. Unpublished paper presented at

Proceedings of the 20th International Conference on Human-Computer Interaction with Mobile Devices and Services. Barcelona, Spain.

Pinter, A. T. *et al.* (2017) *Adolescent Online Safety: Moving Beyond Formative Evaluations to Designing Solutions for the Future*. Unpublished paper presented at Proceedings of the 2017 Conference on Interaction Design and Children. Stanford, California, USA.

Powell, M. A. *et al.* (2018) Sensitive topics in social research involving children, *International Journal of Social Research Methodology*, 21(6), pp. 647-660. doi: 10.1080/13645579.2018.1462882.

Raffel, L. (2020) *Risk Communication: Sexual Predators in Chat Environments*. Master's thesis in Interaction Design, NTNU Gjøvik.

Raffel, L., Bours, P. and Komandur, S. (2020) Attention! Designing a Target Group-Oriented Risk Communication Strategy, *Cham*. Springer International Publishing, pp. 597-604.

Sheehan, K. B. (2002) Toward a Typology of Internet Users and Online Privacy Concerns, *The Information Society*, 18(1), pp. 21-32. doi: 10.1080/01972240252818207.

Smahel, D. *et al.* (2020) EU Kids Online 2020. Survey results from 19 countries: EU Kids Online.

Stickdorn, M. *et al.* (2018) *This is service design doing : applying service design and design thinking in the real world : a practitioners' handbook*. First edition. edn. Sebastopol, CA: O'Reilly.

Tiktok (2021) *Direct messages*. Available at: https://support.tiktok.com/en/using-tiktok/messaging-and-notifications/direct-message-settings (Accessed: 12 April 2021 2021).

Tomitsch, M. *et al.* (2018) *Design, think, make, break, repeat : a handbook of methods*. Amsterdam: B/S Publishers.

Tromp, N. and Hekkert, P. (2019) *Designing for society : products and services for a better world*. London: Bloomsbury Visual Arts.

Van Dam, C. (2001) *Identifying child molesters: Preventing child sexual abuse by recognizing the patterns of the offenders*. Psychology Press.

Ward, T. and Siegert, R. J. (2002) Toward a comprehensive theory of child sexual abuse: A theory knitting perspective, *Psychology, Crime & Law*, 8(4), pp. 319-351. doi: 10.1080/10683160208401823.

Wendel, S. (2014) *Designing for behavior change : applying psychology and behavioral economics*. Sebastopol, Calif: O'Reilly.

Whittle, H. C., Hamilton-Giachritsis, C. E. and Beech, A. R. (2015) A Comparison of Victim and Offender Perspectives of Grooming and Sexual Abuse, *Deviant Behavior*, 36(7), pp. 539-564. doi: 10.1080/01639625.2014.944074.

Wisniewski, P. *et al.* (2015) *"Preventative" vs. "Reactive": How Parental Mediation Influences Teens' Social Media Privacy Behaviors*. Unpublished paper presented at Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work &amp; Social Computing. Vancouver, BC, Canada.

Wisniewski, P. *et al.* (2017a) *Parental Control vs. Teen Self-Regulation: Is there a middle ground for mobile online safety?* Unpublished paper presented at Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing. Portland, Oregon, USA.

Wisniewski, P. *et al.* (2017b) *Parents Just Don't Understand: Why Teens Don't Talk to Parents about Their Online Risk Experiences*. Unpublished paper presented at Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing. Portland, Oregon, USA.

Wong, R. Y. and Mulligan, D. K. (2019) *Bringing Design to the Privacy Table: Broadening "Design" in "Privacy by Design" Through the Lens of HCI*. Unpublished paper presented at Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. Glasgow, Scotland Uk.

Yocco, V. S. (2016) *Design for the mind : seven psychological principles of persuasive design*. Greenwich: Manning.

Zuckerberg, M. (2020) *Starting the Decade by Giving You More Control Over Your Privacy*. Available at: https://about.fb.com/news/2020/01/data-privacy-day-2020/ (Accessed: 12 April 2021 2021).

8 Appendix

8.1 Stakeholder interview guide and questionnaire

Introduction

Briefing participant on details of interview

Hello __ ! I am Nakul. As I mentioned before, I am currently doing my thesis as a part of AiBA project. My specific topic is to understand privacy aspect of children's use of chat apps in various contexts.

Privacy and confidentiality

Audio or video of the discussion is not recorded. The data is gathered only in the form of notes. The raw data will be retained only till the end of the thesis, tentatively July 1, 2021. Findings from this discussion will be included in the report only with your permission.

1. Do you consent to participating in the research?
2. Do I have your permission to include these findings anonymously in the thesis report?

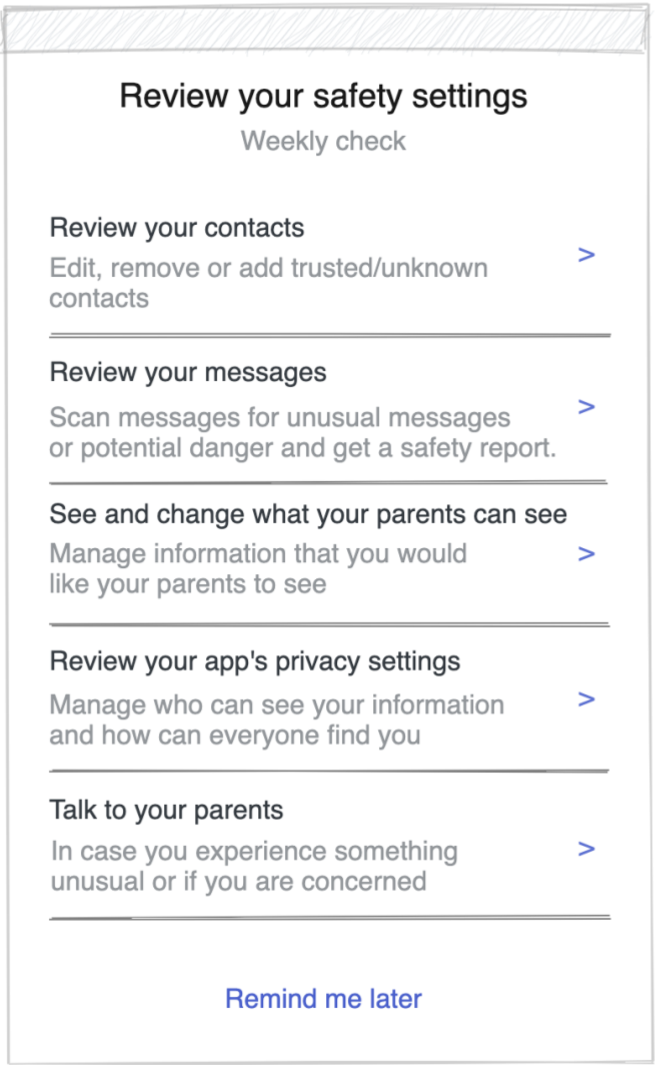
Warm up

1. Could you share a bit about your role in AiBA? What do you look after?

Main Questions – AiBA Stakeholders

1. The way I understand AiBA in an ecosystem as it co-exists along with current chat apps and parental control/mediation software/apps. It helps both of these to be and offer their own functionality.
    a. What are your thoughts on it?
    b. Could you draw the ecosystem diagram roughly on the miro board? (Excluded from the interviews)
2. How do you imagine AiBA in 3-5 years? What shape and form would it be?
3. What are your thoughts on children's privacy when it comes to talking to parents about their day-to-day encounters online?
    a. When parents should start receiving information?
    b. Should parents have access to children's information? If yes, what level of control/access to information should parents have?
    c. How AiBA handles information when a conversation is reported/grooming is detected?
    d. Are there any exceptions to the situation mentioned above?
4. What role should parental control/child safety apps have to protect children's privacy?
    a. When parents prefer using such systems, what challenges, trade-offs, disadvantages they are likely to come across?
    b. How does it/how might it impact a child's interaction with apps or even with parents?

5. A feature analysis of such parental control apps found out that 89% of the apps just focus on monitoring aspect. Why do you think this is the case?
   a. What do you think could be the alternatives?
6. What are your thoughts on parent-child collaboration? What is AiBA's role to become promoters of parent child communication?
   a. What are the challenges, risks involved in this?
7. What are your thoughts on active parental mediation?
8. What are your thoughts on the following concept that tries to increase a child's awareness by reminding them to go through some of the key areas as follows –



Review your safety settings

Weekly check

Review your contacts
Edit, remove or add trusted/unknown contacts >

Review your messages
Scan messages for unusual messages or potential danger and get a safety report. >

See and change what your parents can see
Manage information that you would like your parents to see >

Review your app's privacy settings
Manage who can see your information and how can everyone find you >

Talk to your parents
In case you experience something unusual or if you are concerned >

Remind me later

Main Questions –

1. What are your thoughts on parent-child communication in today's world? How and when do children communicate with their parents?
2. What are your thoughts on children's privacy when it comes to talking to parents about their day-to-day encounters online?
   a. When parents should start receiving information?
   b. Should parents have access to children's information? If yes, what level of control/access to information should parents have?

3. I have this assumption that most parents do not use the parental control apps. Other stakeholders confirmed this assumption that most do not use. What role should parental control/child safety apps have to protect children's privacy?
    a. What are your thoughts on such apps?
    b. How does it/how might it impact a child's interaction with apps or even with parents?
4. A feature analysis of such parental control apps found out that 89% of the apps just focus on monitoring aspect. Why do you think this is the case?
    a. What do you think could be the alternatives?
5. What are your thoughts on parent-child collaboration? What is AiBA's role to become promoters of parent child communication?
    a. What are the challenges, risks involved in this?
6. What are your thoughts on active parental mediation?
7. What are the initiatives from Politi or other social organisations' side? How do they work with children to solve these issues?

Additional optional questions

1. What is the long-term goal of the product?
2. Could you share some of the business goals of AiBA? OR Could you share some of the business aspects of AiBA? What's the next short-term goal of the platform?

Wrap up

Thank you __ for your time. I definitely have a lot of valuable inputs and data. Is it okay if I contact you over email to get a clarification in case of doubts/questions?

Thank you so much!

8.2 Parents' interview guide

8.2.1 Consent form and information letter

Before the interview, information letter was created as per a template given by NSD. This letter was shared with parents before the interview and a consent was obtained. Similar consent form was created for focus group and surveys and were circulated via school internal system.

Vil du delta i forskningsprosjektet - "AiBA – Trygghet for barn i chatterom"

Vil du delta i et forskningsprosjekt om trygghet for barn i chatterom? Formålet er å forstå hvordan barn bruker chat-apper og hvordan vi kan designe en løsning som beskytter barn i chatterom mot overgripere pånett. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål

Dette prosjektet er en del av masteroppgave i interaksjonsdesign på Norges teknisk-naturvitenskapelige universitet (NTNU). Denne masteroppgaven vil bli innlemmet i AiBA (Author Input Behavioral Analysis) prosjektet veiledet av Patrick Bours. AiBA-prosjektets overordnede mål er å beskytte barn på nettet mot seksuelle overgripere, grooming og nettmobbing gjennom å identifisere og forhindre grooming i online chatterom. Det tar sikte på å identifisere falske profiler i chatte-applikasjoner. Denne studien er ment å skaffe innsikt i kunnskapen om grooming og seksuelle overgripere på nettet. Gjennom dette er målet å utvikle en måte å advare barn i live chatte-samtaler om potensiell fare. Bevissthetskampanjer og å se påhvordan foreldre og barn kan informeres om potensielle risikoer på nett er en viktig del av dette prosjektet.

Hvem er ansvarlig for forskningsprosjektet?

Norges teknisk-naturvitenskapelige universitet (NTNU) i Gjøvik er ansvarlig for prosjektet.

Hvorfor får du spørsmål om å delta?

For å kunne gjøre denne studien og finne relevante deltakere for datainnsamling, har lokale skoler i området blitt kontaktet og et samarbeid med barneskolene er etablert gjennom rektorene og NTNU. Målgruppen her er barna i 5. til 7. klasse og deres foreldre. Det er blant annet etablert kontakt med Kopperud (Gjøvik) og Vestre Toten Ungdomsskole (VTU i Raufoss) Målgruppen her er barna i 8. til 9. klasse og deres foreldre.

Hva innebærer det for deg å delta?

Utvalg 1-Foreldre til barn i 5. til 9. klasse - intervju

- Hvis du velger å delta i prosjektet, innebærer det at du vil delta i et dybdeintervju. Det vil ta mellom 45 til 60 minutter. Intervjuet inneholder spørsmål om barns chattevaner og dine erfaringer rundt tema. Dine svar fra i intervjuet blir registrert som notater og det vil bli tatt opp lyd av samtalen. Lydopptakene brukes i analysearbeidet i etterkant av intervjuene og vil deretter slettes. På grunn av koronarestriksjoner så vil intervjuene mest sannsynlig bli gjennomført digitalt via Zoom eller Microsoft Teams.

Det er frivillig å delta

Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykket ditt uten å oppgi noen grunn. Alle dine personopplysninger vil da bli slettet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller velger å trekke deg ved en senere anledning.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger

Vi vil bare bruke opplysningene om deg til formålet vi har fortalt om i dette skrivet. Vi behandler alle opplysninger konfidensielt og i samsvar med personvernregelverket.

Det er kun prosjektansvarlig Patrick Bours og student Marit Sylstad og Nakul Pathak ved NTNU som vil ha tilgang til dataene i prosjektet.

Utvalg 1

Det er kun prosjektansvarlig Patrick Bours og student Marit Sylstad og Nakul Pathak ved NTNU som vil ha tilgang til dataene utvalg 1 før de anonymiseres. Navnet til utvalg 1 og kontaktopplysningene dine vil erstattes med en kode som lagres på egen navneliste adskilt fra øvrige data. Dette lagres på trygg forskningsserver med passord. I publikasjoner vil dataene være anonymisert. Det er likevel en mulighet for at du gjenkjenner egne uttalelser fra intervjuet.

Du som testperson vil ikke, kunne identifiseres (direkte eller indirekte) i oppgaven eller øvrige publikasjoner fra prosjektet.

Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?

Opplysningene anonymiseres når prosjektet avsluttes, noe som etter planen er ved utgangen av juli 2021. Personopplysninger, koblingsnøkkelen og opptak vil da slettes, og kun det anonymiserte datamaterialet beholdes.

Dine rettigheter

Så lenge du kan identifiseres i datamaterialet, har du rett til:

- - innsyn i hvilke personopplysninger som er registrert om deg, og å få utlevert en kopi av opplysningene,
- - å få rettet personopplysninger om deg,
- - å få slettet personopplysninger om deg, og
- - å sende klage til Datatilsynet om behandlingen av dine personopplysninger.

Hva gir oss rett til å behandle personopplysninger om deg?

Vi behandler opplysninger om deg basert på ditt samtykke.
På oppdrag fra Norges teknisk-naturvitenskapelige universitet (NTNU) har NSD – Norsk senter for forskningsdata AS vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Hvor kan jeg finne ut mer?

Hvis du har spørsmål til studien, eller ønsker å benytte deg av dine rettigheter, ta kontakt med: Norges teknisk-naturvitenskapelige universitet (NTNU) ved Patrick Bours.

- Forskningsveilederen kan kontaktes på patrick.bours@ntnu.no. Hvis du har andre praktiske spørsmål, kan du kontakte student Marit Sylstad maritsyl@stud.ntnu.no og Nakul Pathak nakulp@stud.ntnu.no.
- Vårt personvernombud er Thomas Helgesen, thomas.helgesen@ntnu.no.

Hvis du har spørsmål knyttet til NSD sin vurdering av prosjektet, kan du ta kontakt med:

- NSD – Norsk senter for forskningsdata AS på epost (personverntjenester@nsd.no) eller på telefon: 55 58 21 17.

Med vennlig hilsen

Patrick Bours	**Marit Sylstad**	**Nakul Pathak**
Forsker/veileder	Student	Student

8.2.2 Interview guide and questionnaire

Introduction

Hello __!

We are Marit and Nakul. We are studying masters in interaction design here at NTNU in Gjøvik.

We are conducting this research to understand children’s chat app usage and your thoughts on the topics.

We will use the findings from this discussion in our research to come up with better solutions that protects children’s privacy and increases children and parent’s awareness.

We have few questions for you, the questions are open-ended and there is no right or wrong answer. So feel free to say whatever comes to your mind that you feel is relevant. You can stop the discussion if you feel uncomfortable or don’t wish to continue.

About privacy and confidentiality

We would like to share few details about how we handle data.

All the data collected is in the form of notes, sound recording and will be only shared with research supervisor from NTNU. The data is safely stored. We will anonymise all the raw data once the analysis is completed. The raw data will only be retained until this thesis is completed, tentatively by end of July 2021.

Have you signed the consent document?

In case you have any other questions, you can reach us at nakulp@stud.ntnu.no or maritsyl@stud.ntnu.no . The thesis/research supervisor can be contacted at patrick.bours@ntnu.no.

The research is part of the AiBA (Author Input Behavioural Analysis) project, which monitors chat conversations through behavioural biometrics and text analysis to warn users about false identities and suspicious behaviour. The AiBA project is conducted by the Norwegian Biometry Laboratory which is part of the Department of Information Security and Communication Technology at NTNU Gjøvik.

Shall we continue?

Do you have any questions before we start?

Warm-up questions and Introduction (10 min)

1. Can you tell me about yourself?
2. Hvilken klassetrinn går barna dine på?
3. What do you usually use the internet for? (Online banking? Online newspapers? Facebook?)
4. What type of devices do you use regularly?
    a. Smartphone/Mobile
    b. Laptop or PC
    c. Tablet/iPad
    d. Game console (PlayStation, Nintendo Switch, Xbox etc.)
    e. Smart watch - Fitbit, Apple watch, Garmin etc.
    f. None/prefer not to say
5. How much time do you spend online each day outside of work?
    a. Less than an hour
    b. 1-2 hours
    c. 2-3 hours
    d. More than 3 hours
6. What social media do you use? (Facebook, Snapchat, Instagram, TikTok, YouTube or any other)
7. Have you experienced attempts of internet scams/virus?
    a. If yes, how did you react to it?

Main question (20 – 25 min)

For elaboration of topics that arise, spontaneous follow-up questions can be asked along the way.

Part 1 – Awareness on safe internet usage

8. Have you received any information on – how can you make a child's internet usage safe? For instance, Nettvett etc.
9. (Optional) Where would you like to get information and advice on how to help and support your child on the internet and keep him or her safe?
10. How do you talk to your kids about safe internet use and the dangers they can face online? (hints if asked: Namely - Safe use of passwords, sharing private information/photos, predators online etc.)
    a. Do you think your child(ren) is aware about risks online?

Part 2 – How parents monitor a child's usage

11. Are your kids on social media?
    a. Do you follow them on all those platforms?
12. Can you describe your main concerns regarding your children and the dangers they may face online? Bullying, grooming etc..
13. Can you describe how if you use any digital apps/tools such as parental controls software to keep your children safe online? How you keep track of what your kids are doing online/control time spent?
    a. What are its pros and cons? What could be done better?
    b. Have you faced any challenges?
    c. Is it anything you think is difficult or too complex to talk to you child about

Part 3 – Parents' preferences of receiving information

14. Are you aware about concept of grooming/predators?

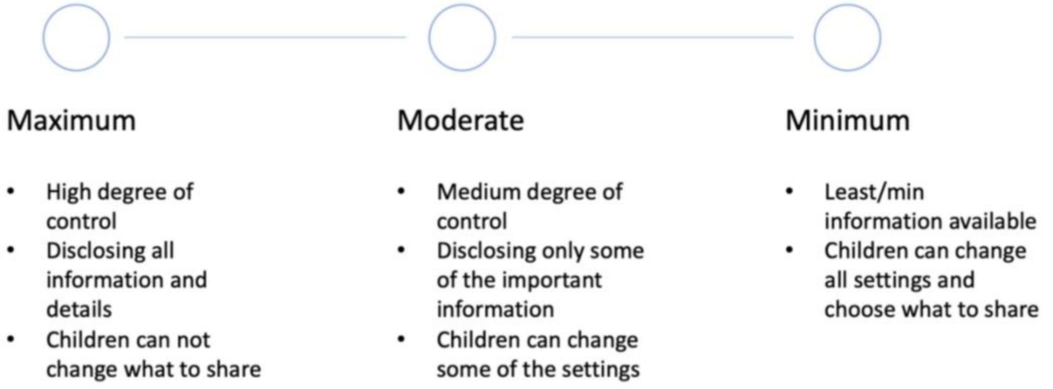
    Grooming is when someone builds a relationship, trust and emotional connection with a child or young person so they can manipulate, exploit and abuse them.

    Grooming er prosessen hvor en voksen blir venner med, og oppretter en emosjonell kontakt med et barn, for så å avtale et møte med det slik at det vil bli mulig for den voksne å ha seksuell omgang med barnet.

15. As a parent what kind of information would you like to receive about the risks of online grooming/ predators?
16. In your opinion what is the best way to protect children from online predators?

Part 4 – Privacy and thoughts on privacy solution - Personvern

17. How do you talk about privacy with your child? If yes, how often?
    a. How would you approach this topic?
18. What do you think about children's privacy?
    a. In case if he/she would like to share an online experience, what do they like sharing/talking about? What do they prefer keeping secret?
19. (Optional) What do you think he/she thinks about privacy with respect to these topics?
20. What do you thoughts on – safety review system that is built into their chat apps? (The question was excluded for most of the participants, instead the low fidelity prototype was tested)
    a. Description – Imagine a system which gives you warning about potential sexual grooming in chats. The system protects the child and keeps parents informed about potential dangers. With help of some features, a child can have a conversation with parent(s) about his/her experiences online. The system can also protect child's privacy in cases where there is potential grooming. A child can select what parents can see and know.
    b. If you as a parent are to choose what you would like to see, what would you prefer from the following?



Maximum

- High degree of control
- Disclosing all information and details
- Children can not change what to share

Moderate

- Medium degree of control
- Disclosing only some of the important information
- Children can change some of the settings

Minimum

- Least/min information available
- Children can change all settings and choose what to share

Wrap up (Summary and clarification 5-10 mins)

1. Summarize the main findings
2. Do you want to elaborate on some of what we have said? Would you like to add something to the discussion so far?

Thank you for taking time out. We have gotten very valuable information out from this discussion. It was nice talking to you. Have a nice day!

8.3 Survey questionnaire

Introduction

Hello __!

We are Marit and Nakul. We are studying masters in interaction design here at NTNU in Gjøvik. The purpose is to understand how children use chat apps.

We will use the data to create better system that –

1. Protects children's privacy
2. Keep children safe online
3. Increase parent's and children's awareness

About privacy and confidentiality

We would like to share few details about how we handle data.

We are not gathering any personal information that identifies you individually. The data is anonymized and safely stored. Your participation is completely voluntary, and you can stop the survey at any time if you feel uncomfortable or don't wish to continue.

In case you have any other questions, you can reach us at nakulp@stud.ntnu.no or maritsyl@stud.ntnu.no . The thesis/research supervisor can be contacted at patrick.bours@ntnu.no.

Thank you for helping us.

Part 1 – About you

We would like to know a little bit about you and how you use internet and devices.

1. Are you a
    a. Girl
    b. Boy
    c. Other
    d. Prefer not to say.
2. What grade are you in?
    a. 5th grade
    b. 6th grade
    c. 7th grade
    d. 8th grade
    e. 9th grade
3. Do you use any of these digital devices? (Select that applies) / Har du noe av dette hjemme?
    a. Smartphone/mobile
    b. Tablet /Nettbrett (IPad el.)
    c. PC/Laptop/Gaming PC
    d. Spill konsoll (Playstation, Nintendo Switch, Xbox etc.)
    e. Smart Kids watch /Klokke du kan ringe med
4. How much do you use each of the following apps? For each app, options are - More than 2 hours a day, 1-2 hours a day, less than an hour, I don't use this app, I'm not allowed to use this app, don't want to say
    a. Facebook
    b. Snapchat
    c. Instagram

    d. TikTok
    e. Discord
    f. Messenger
    g. Messenger kids
    h. Telegram
    i. Others (please specify -)
5. How much do you play any of these online games: (For each app, options are - More than 2 hours a day, 1-2 hours a day, less than an hour, I don't use this app, I'm not allowed to use this app, don't want to say)
    a. Fortnite
    b. Minecraft
    c. Roblox
    d. Movie Star Planet
    e. MarioKart Tour
    f. Other: ____ (Removed from the final survey)

Part 2 – Your experiences on chat apps

A chat conversation can happen in various apps such as Snapchat, Facebook Messenger, Discord, online chatrooms such as www.Chatroulette.com , during online games such as Fortnite, MovieStarPlanet FIFA, Roblox, Minecraft and so on.

Remember that other people will not know that these answers are yours, so please answer as best you can. If you don't know or don't want to answer any of the questions, just answer "don't remember, I don't know or rather not say.

6. Rate the following statements (1 – Least agree, 5 - Highly Agree)
    a. I have a lot of contact with my friends on social media
    b. In social media, I meet people with same interest as me
    c. I have regretted sharing something on social media or in the chat
    d. I feel like I am more myself online than in real life
7. What do you usually do when someone asks you to become "friends" or follow you on social media? Tick all that are right for you
    a. I accept everyone
    b. I accept if we are the same age
    c. I accept if we have mutual friends
    d. I only accept if I know them
    e. I only accept if my parents say it's ok
    f. I do not accept anyone
    g. I don't know
8. Have you ever had contact on the internet with someone you have not met in real life/face-to-face before?
    a. Yes, often
    b. Yes, once or twice
    c. No, never
    d. Don't know/ don't remember
9. In the past have you ever met anyone face-to-face that you first got to know online?
    a. Yes, often
    b. Yes, once or twice
    c. No, never
    d. Don't know/ don't remember

Routing if yes;

10. The LAST time you met someone face-to-face that you first got to know online or on a phone, how did you feel about it?
    a. I was happy
    b. I was not happy or upset
    c. I was a little upset
    d. I was fairly upset
    e. I was very upset
    f. Prefer not to say
11. The LAST time you met someone face-to-face that you first got to know online or on a phone, how old was the person you met? (Choose one answer)
    a. I met with someone about my age
    b. I met with someone younger than me
    c. I met with a teenager older than me
    d. I met with an adult

12. Rate following statements based on your experiences (1-Never 5- Many times)
    a. I have been asked for address, phone number or password during a chat conversation with someone I don't know
    b. I have been asked to share a photo of myself during a chat conversation with someone I don't know
    c. I have been asked to share a sexual or naked photo of myself (picture or video) someone I don't know
    d. I have been asked to share a sexual or naked photo of myself (picture or video) during a chat with someone I know

Routing if not never

13. Last time you were asked for private or sexual information online -What did you do?
    a. Nothing in particular
    b. I blocked the person
    c. I talked to a friend about it
    d. I am still in contact with the person
    e. I reported the person
    f. I didn't tell anyone
    g. I told my parents/a trusted adult
    h. I reported the person using the applications reporting function
    i. don't know/ don't remember

(The section headings were changed in the final survey)

Part 3 – Privacy towards outside world

1. What is the best way to protect children online? What do you think is most important to be safe in chat apps? What will make you feel safe while chatting? What is needed to be safe in chatting?
    a. What do you need to feel safe, while chatting online or using chat apps?
2. Rate statements from 1 to 5 (1- least applicable, 5-most applicable and not sure/don't know)
    a. I like keeping my apps/software up-to date.
    b. I often check my social media account settings (including privacy settings) regularly.
    c. I know what information I am sharing to my friends/followers/everyone.
    d. I know what information app is gathering about me.
    e. I know how to keep my data safe.

Part 4 – privacy and keeping parents informed about daily usage

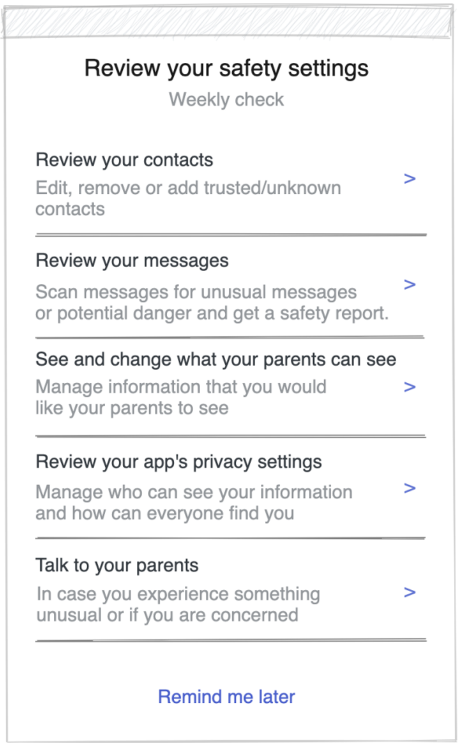
3. Rate following statements based on your understanding and experiences (1-Least applicable 5- most applicable)
    a. My parents have told me about risks in using chat apps.
    b. I follow the rules my parents have made about using chat apps
    c. I talk to my parents about conversations I have had over chat apps.
    d. I like to discuss my negative/strange experiences online (or on chat apps) with my parents.
    e. I think a chat app can help me discuss dangers/negative experiences on chat apps with my parents.
    f. I feel the need to talk to my parents, if I come across something strange/negative/unusual.
    g. I find it difficult to talk to my parents about my experiences in chat apps.
    h. I can handle the situation by myself after experiencing something unusual/concerning on chat apps.

Part 5 – Questions around privacy check solution and questions around it

Imagine your chat apps (or social media apps) with additional features. These features will keep children safe and detect risks. For example, the system can identify if a child is talking to someone who is having fake profile or someone trying to get private information for wrong purposes.

The app will send a reminder every 15 days to remind you to go through some things –

1. **Review messages** – You can scan messages and see if there are any risks. System can highlight chats with risk, and you can take action on it.
2. **Review your app's privacy** – You can control and change who can find you, contact you and see your profile information.
3. **Review your contacts** – With this you can go through your contacts/follower list. You can edit/remove unknown contacts or add trusted contacts.
4. **Edit what your parents can see** – In case there is risk which requires action, your parents might be notified. However, you can decide what information they can see along with the warning.
5. **Talk to your parents** – If you experience something negative or strange, you can talk to your parents about it through chat.



Review your safety settings

Weekly check

Review your contacts

Edit, remove or add trusted/unknown contacts >

Review your messages

Scan messages for unusual messages or potential danger and get a safety report. >

See and change what your parents can see

Manage information that you would like your parents to see >

Review your app's privacy settings

Manage who can see your information and how can everyone find you >

Talk to your parents

In case you experience something unusual or if you are concerned >

Remind me later

1. Please rate following statements on a scale of 1-least useful to 5 -most useful
    a. Review your contacts
    b. Review your messages
    c. See and change what your parents can see
    d. Review your app’s privacy settings
    e. Talk to your parents
    f. I find this solution useful.
    g. I think this will help me to talk about my experiences with my parents.
    h. I feel this can protect and make me aware about dangers.

Thank you note

If you experience something negative, it is important to talk to someone you trust.

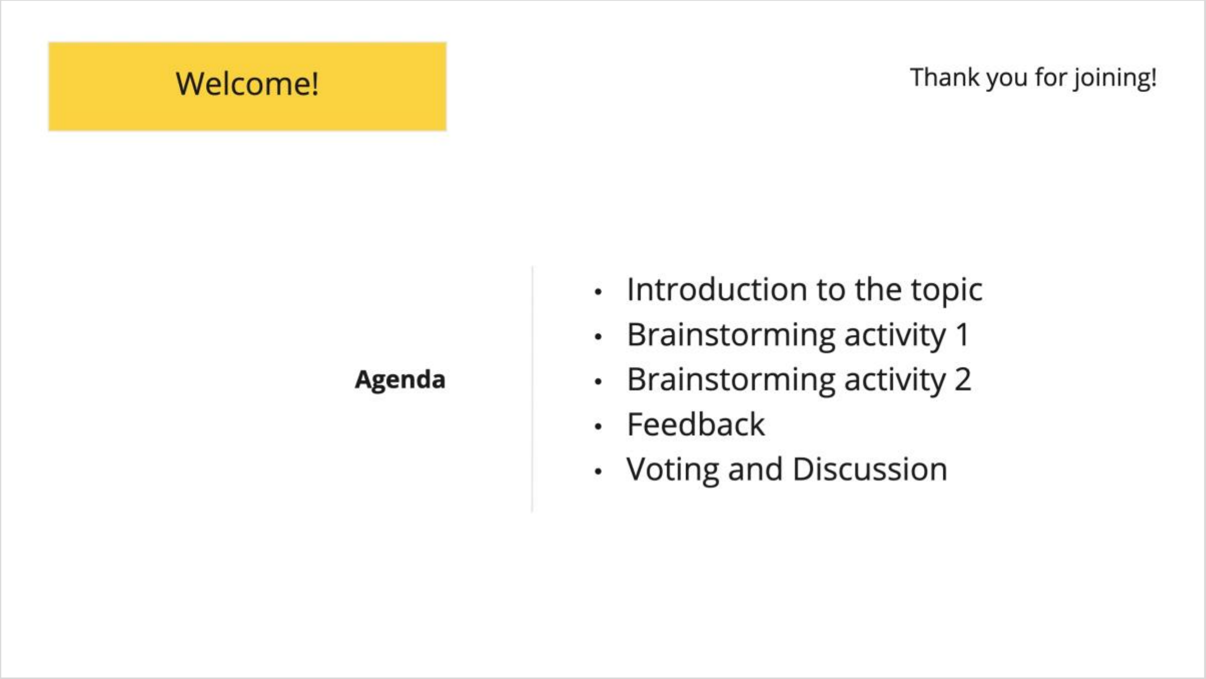
You can also call “Alarmtelefonen for barn og unge” on **116 111**

- Alarmtelefonen er en gratis telefon for barn og unge som er utsatt for vold, overgrep og omsorgssvikt. Alarmtelefonen er døgnåpen. https://www.116111.no/

You have given us valuable information and inputs. This will really help make children’s lives safer and better. Thank you for your time. Have a great day ahead!

8.4 Focus group with designers

This section contains all the details that were part of the focus group with designers.

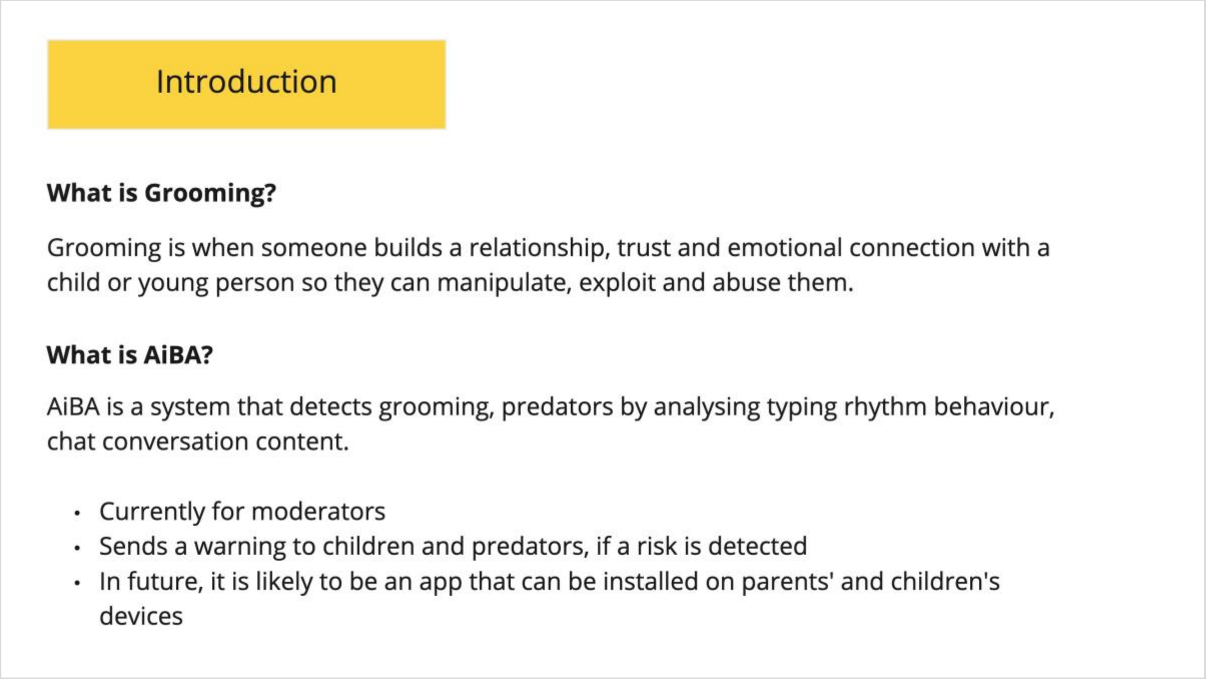


Welcome!

Thank you for joining!

Agenda

- Introduction to the topic
- Brainstorming activity 1
- Brainstorming activity 2
- Feedback
- Voting and Discussion



Introduction

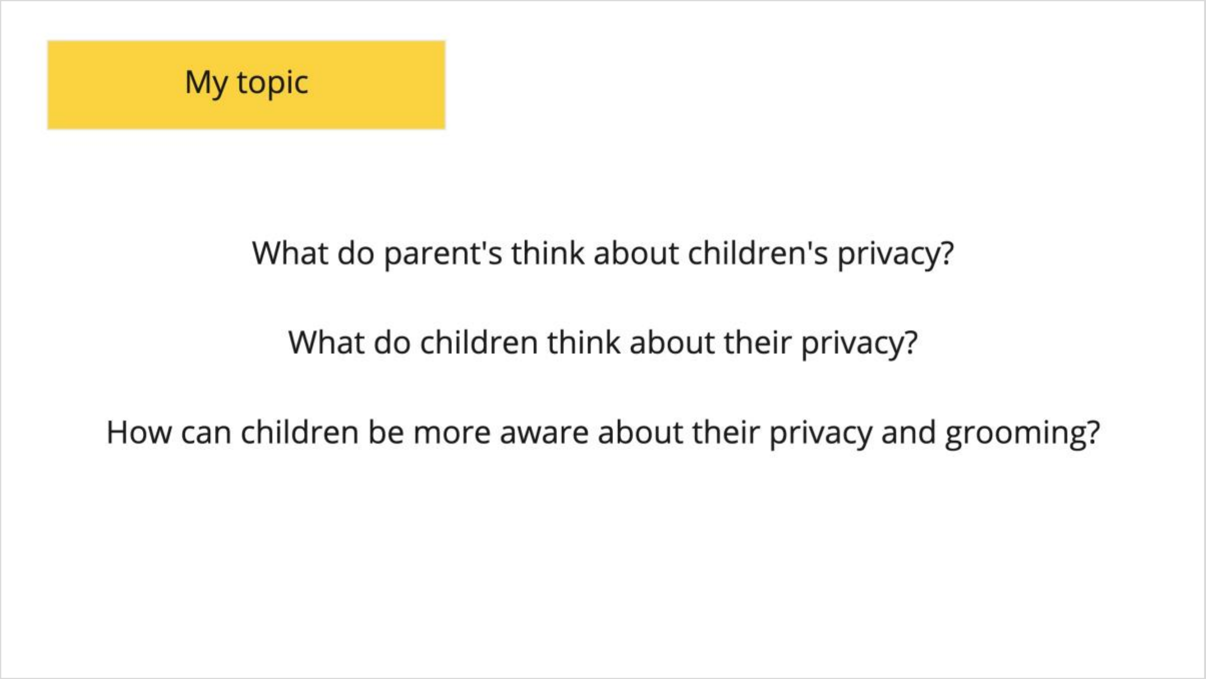
What is Grooming?

Grooming is when someone builds a relationship, trust and emotional connection with a child or young person so they can manipulate, exploit and abuse them.

What is AiBA?

AiBA is a system that detects grooming, predators by analysing typing rhythm behaviour, chat conversation content.

- Currently for moderators
- Sends a warning to children and predators, if a risk is detected
- In future, it is likely to be an app that can be installed on parents' and children's devices

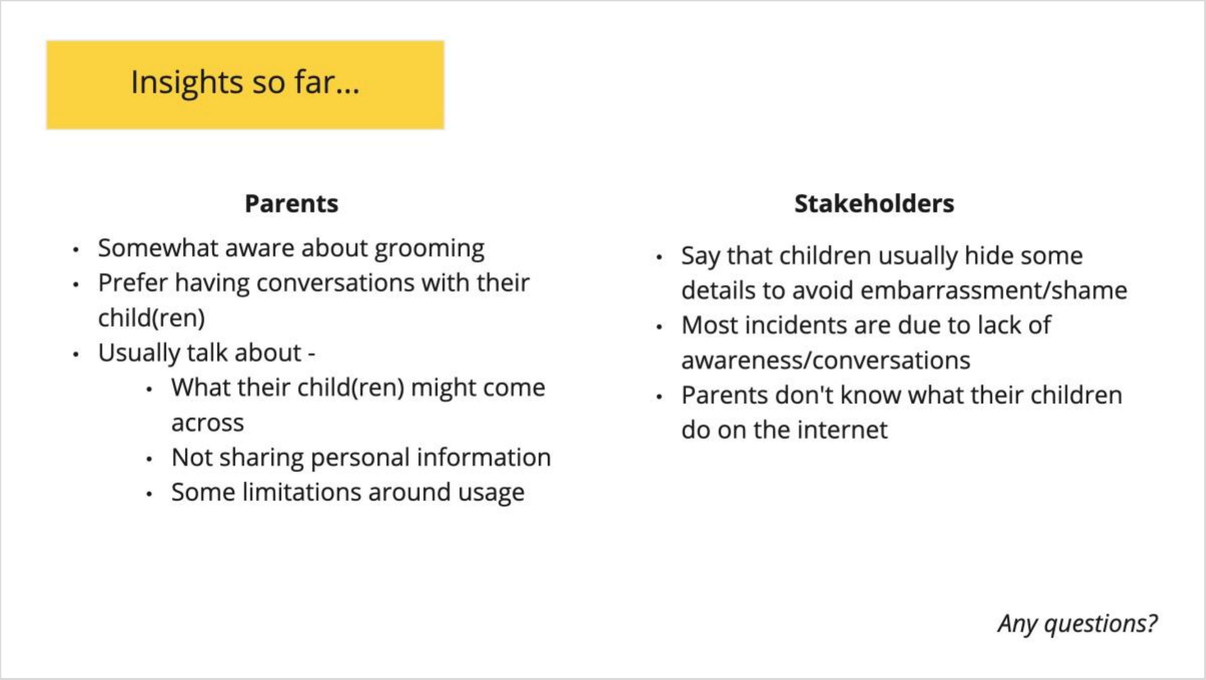


My topic

What do parent's think about children's privacy?

What do children think about their privacy?

How can children be more aware about their privacy and grooming?



Insights so far...

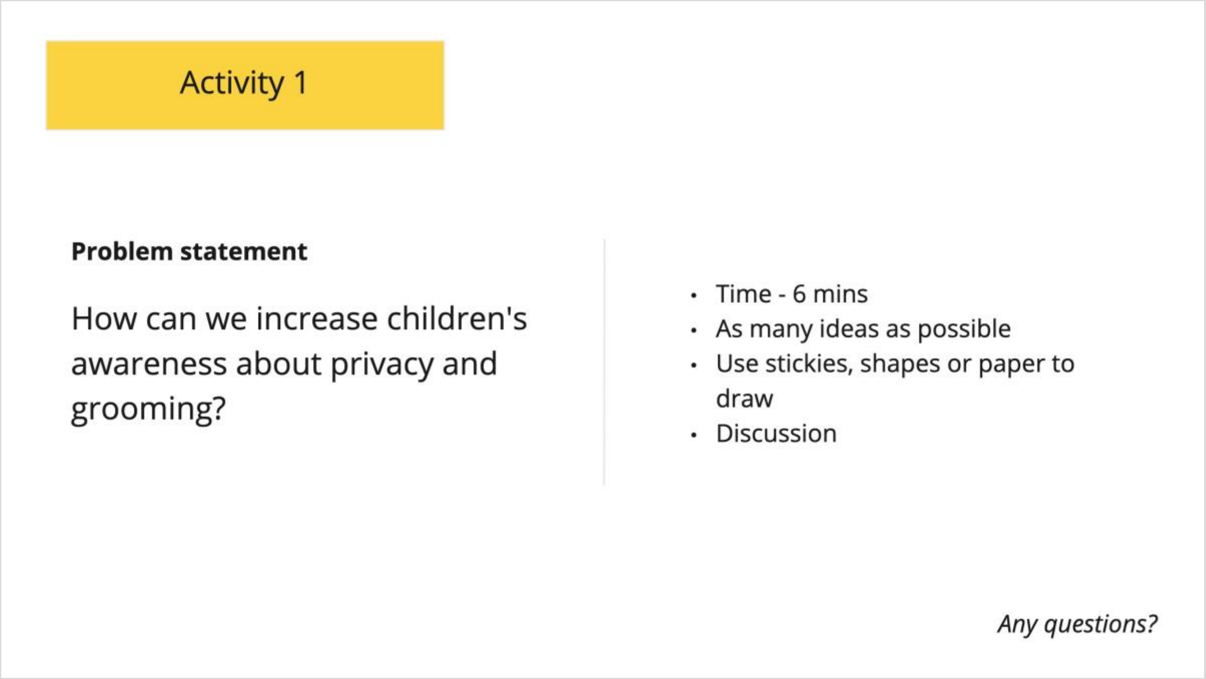
Parents

- Somewhat aware about grooming
- Prefer having conversations with their child(ren)
- Usually talk about -
    - What their child(ren) might come across
    - Not sharing personal information
    - Some limitations around usage

Stakeholders

- Say that children usually hide some details to avoid embarrassment/shame
- Most incidents are due to lack of awareness/conversations
- Parents don't know what their children do on the internet

Any questions?



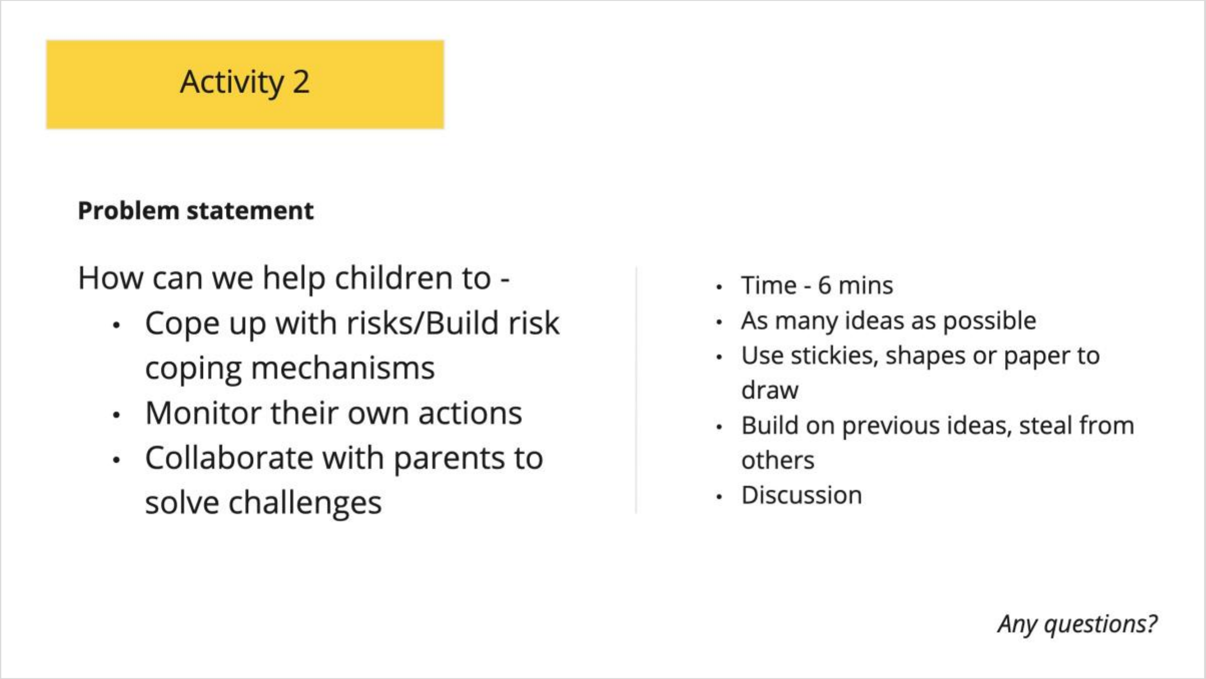
Activity 1

Problem statement

How can we increase children's awareness about privacy and grooming?

- Time - 6 mins
- As many ideas as possible
- Use stickies, shapes or paper to draw
- Discussion

Any questions?



Activity 2

Problem statement

How can we help children to -

- Cope up with risks/Build risk coping mechanisms
- Monitor their own actions
- Collaborate with parents to solve challenges

- Time - 6 mins
- As many ideas as possible
- Use stickies, shapes or paper to draw
- Build on previous ideas, steal from others
- Discussion

Any questions?

Activity 3

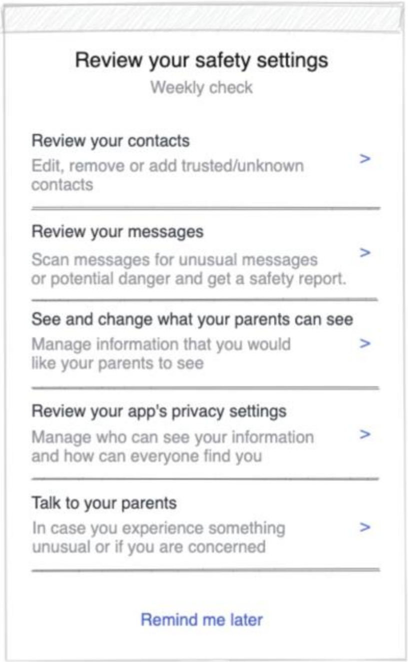
Feedback

What are your thoughts on this solution?

- A reminder for children in their chat app

- Time - 5 mins
- Write your feedback
- Building on this idea
- Draw/use wireframe, icon library
- Discussion

Any questions?



Review your safety settings

Weekly check

Review your contacts
Edit, remove or add trusted/unknown contacts >

Review your messages
Scan messages for unusual messages or potential danger and get a safety report. >

See and change what your parents can see
Manage information that you would like your parents to see >

Review your app's privacy settings
Manage who can see your information and how can everyone find you >

Talk to your parents
In case you experience something unusual or if you are concerned >

Activity 3

Voting on ideas

Vote on your favorite ideas across all activities.

- Time - 5 mins
- Discussion

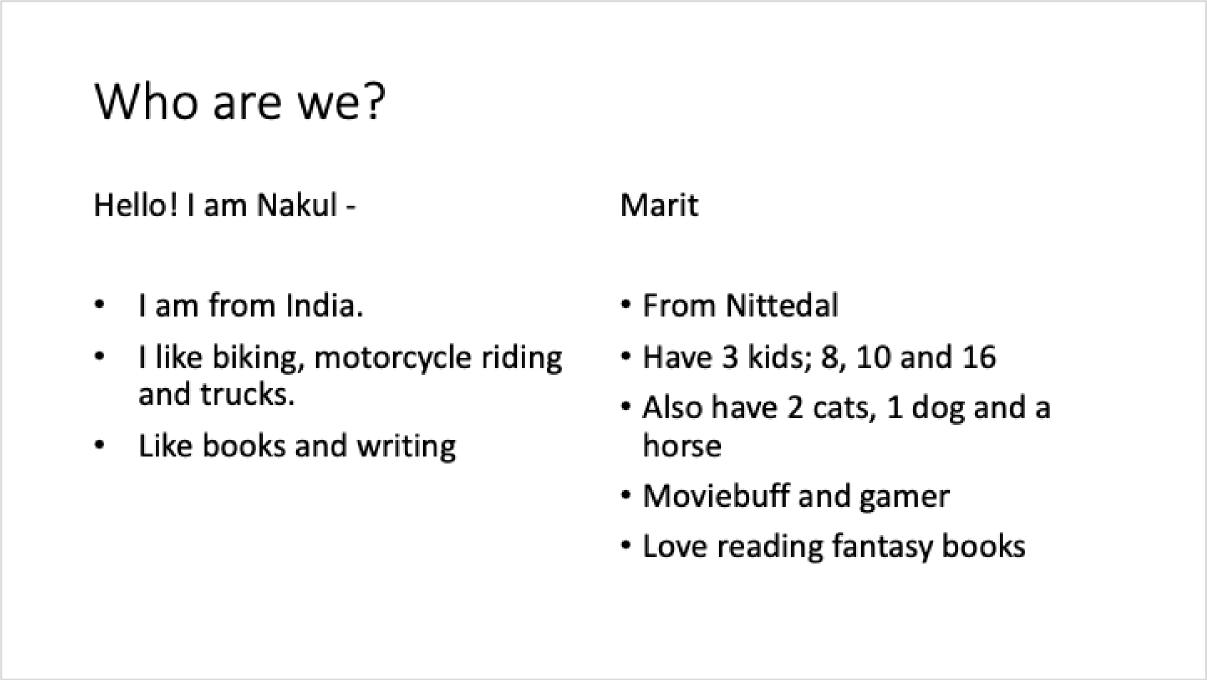
Any questions?

8.5 Focus group with children questionnaire

This section contains all the details that were part of the focus group with children.

Focus Group
Kopperud skole

AiBA Project



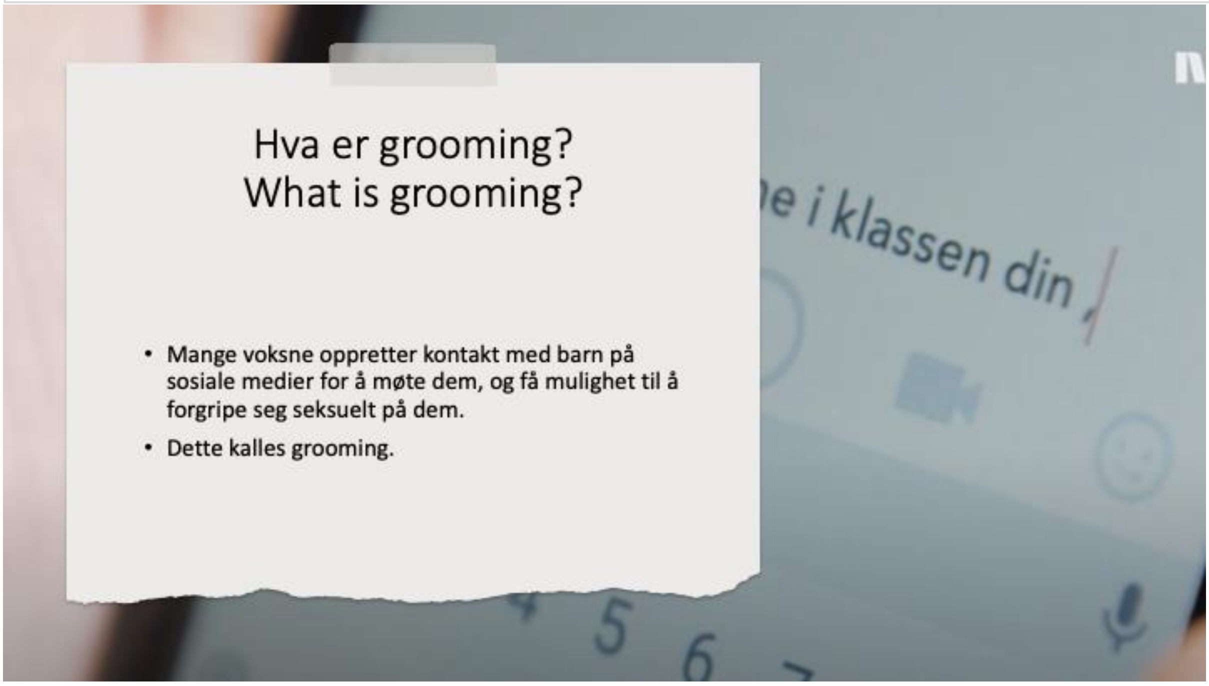
Who are we?

Hello! I am Nakul -

- I am from India.
- I like biking, motorcycle riding and trucks.
- Like books and writing

Marit

- From Nittedal
- Have 3 kids; 8, 10 and 16
- Also have 2 cats, 1 dog and a horse
- Moviebuff and gamer
- Love reading fantasy books



Hva er grooming?
What is grooming?

- Mange voksne oppretter kontakt med barn på sosiale medier for å møte dem, og få mulighet til å forgripe seg seksuelt på dem.
- Dette kalles grooming.

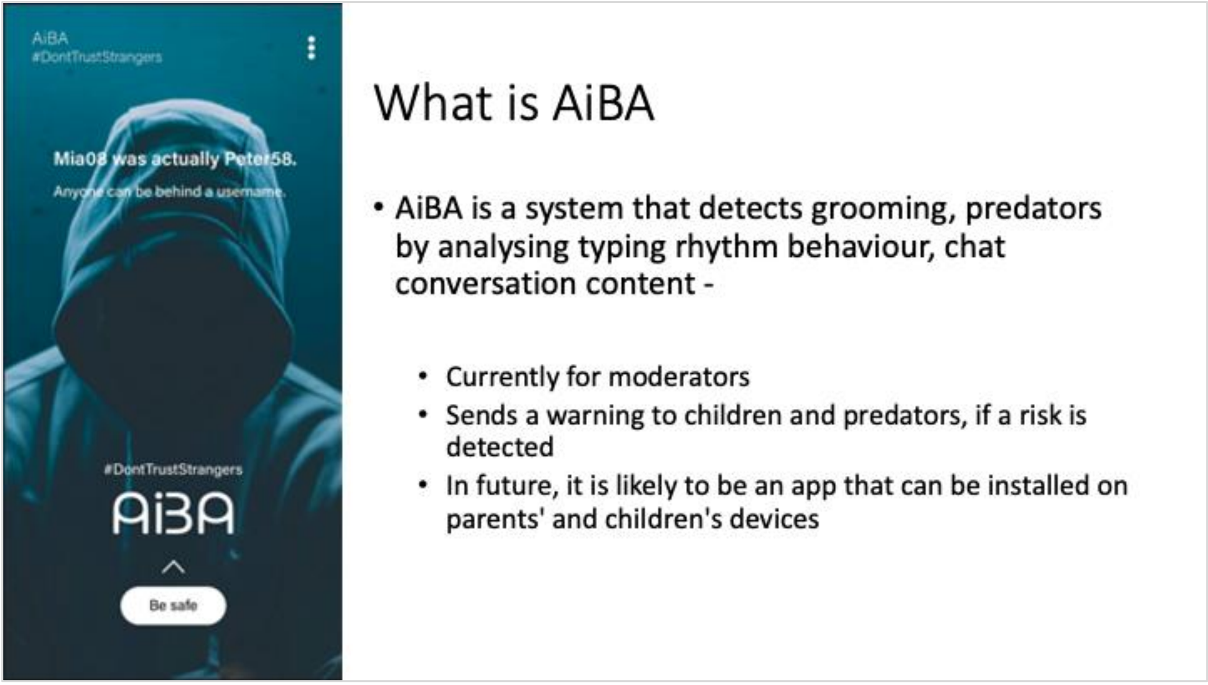
e i klassen din

karlerik31

Blir skuffet hvis jeg ikke får se mer :(
Og hvis jeg blir skuffet, blir jeg nødt til å dele bildet ditt med flere.
Kanskje foreldrene dine?
Du får 10 sekunder på deg
10
9

Det er viktig å si i fra

https://youtu.be/x9MOhsd86Xc

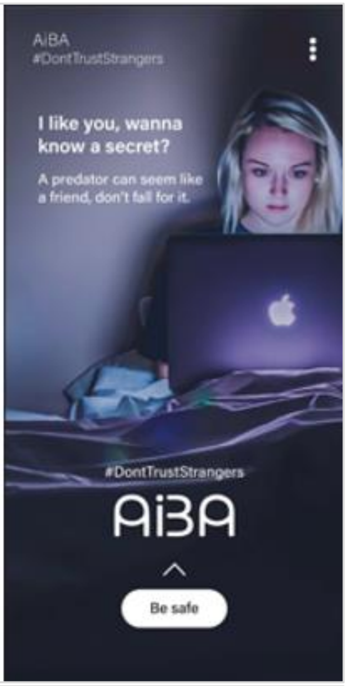

AiBA
#DontTrustStrangers
Mia08 was actually Peter58.
Anyone can be behind a username.
#DontTrustStrangers
AiBA
Be safe

What is AiBA

- AiBA is a system that detects grooming, predators by analysing typing rhythm behaviour, chat conversation content -
    - Currently for moderators
    - Sends a warning to children and predators, if a risk is detected
    - In future, it is likely to be an app that can be installed on parents' and children's devices

Ice-breakers

- Tell me a bit about yourself? Siblings? Pets? Hobbies
- How do you communicate with your friends?
- If you could only be on one social network for a week, which would you choose and why?
- What would it be like to be without the internet for a whole week?

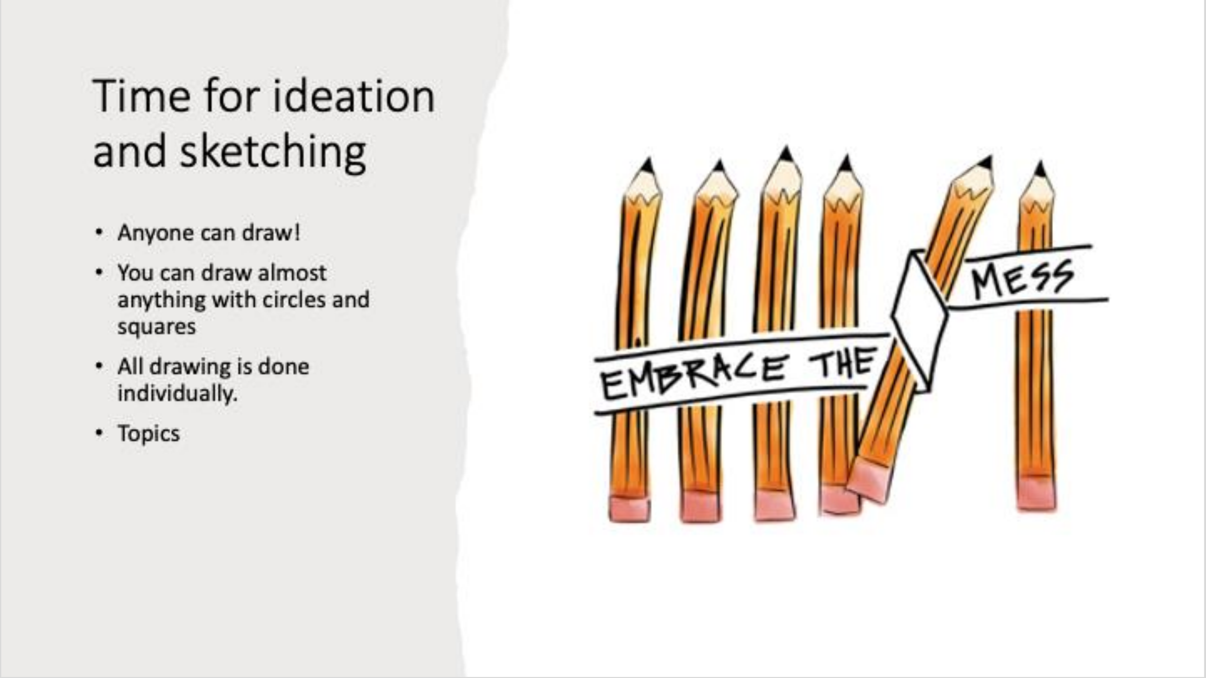

AiBA
#DontTrustStrangers
I like you, wanna know a secret?
A predator can seem like a friend, don't fall for it.
#DontTrustStrangers
AiBA
Be safe

Questions about online risks

1. How safe do you feel online on a scale of 1-10? Why?
2. Is it okay to meet someone you have met online in real life?
3. What do you do if someone you do not know contacts you online?
4. Where is the limit to what is okay to say or do online?
5. What do you think one should do if a friend is treated badly online?
6. Do you feel you can talk to your parents about what you are experiencing online?

Work in groups

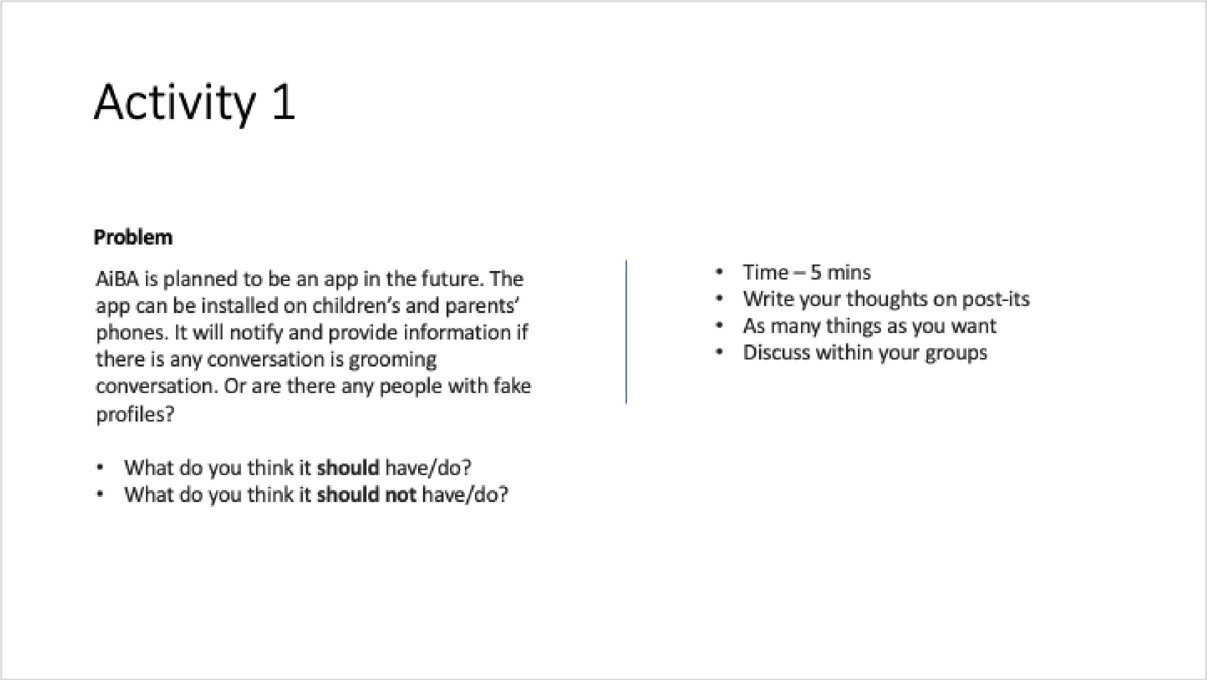
- Get divided in groups of 3.
- Draw a sketch of a person to your left in 45 seconds.
- Decide your group's superpower and draw a mascot in 2 mins.



Time for ideation and sketching

- Anyone can draw!
- You can draw almost anything with circles and squares
- All drawing is done individually.
- Topics

EMBRACE THE
MESS



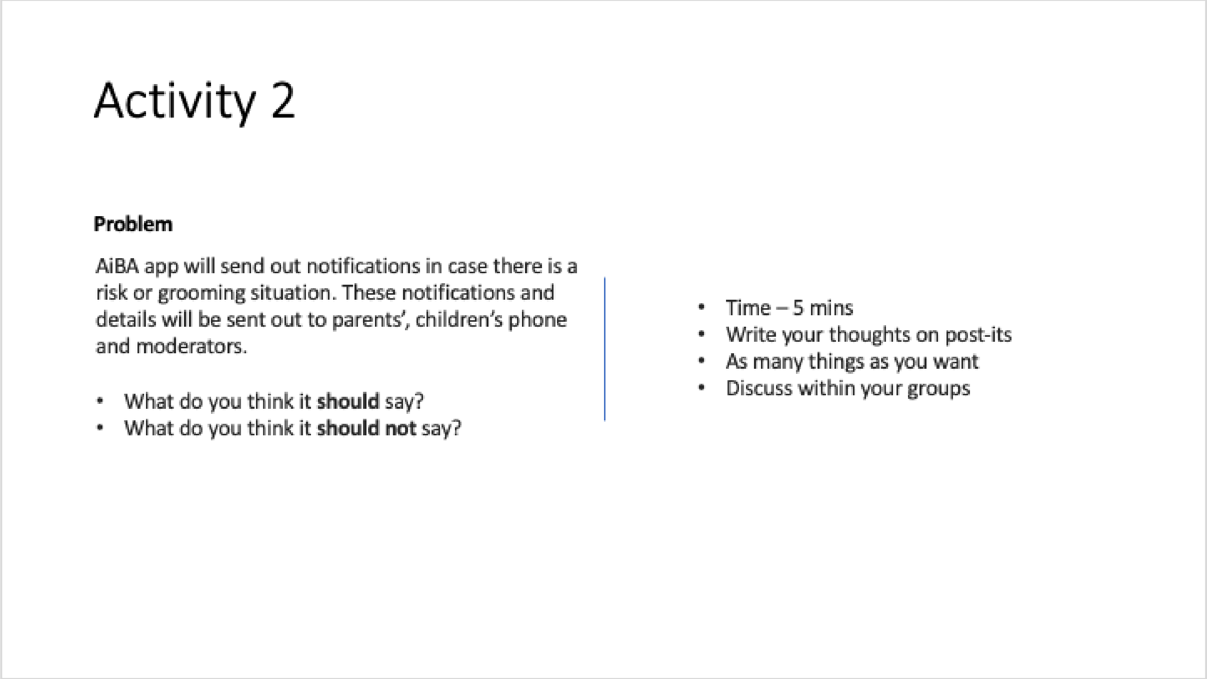
Activity 1

Problem

AiBA is planned to be an app in the future. The app can be installed on children's and parents' phones. It will notify and provide information if there is any conversation is grooming conversation. Or are there any people with fake profiles?

- What do you think it **should** have/do?
- What do you think it **should not** have/do?

- Time – 5 mins
- Write your thoughts on post-its
- As many things as you want
- Discuss within your groups



Activity 2

Problem

AiBA app will send out notifications in case there is a risk or grooming situation. These notifications and details will be sent out to parents', children's phone and moderators.

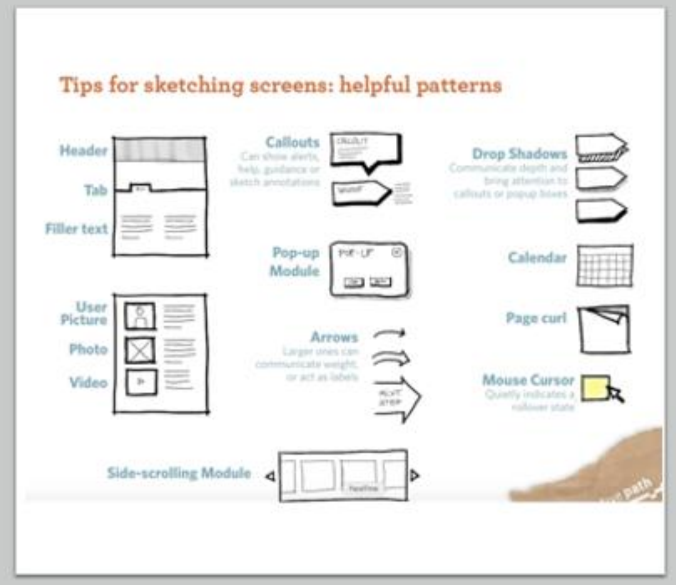
- What do you think it **should** say?
- What do you think it **should not** say?

- Time – 5 mins
- Write your thoughts on post-its
- As many things as you want
- Discuss within your groups

Do you want a break?

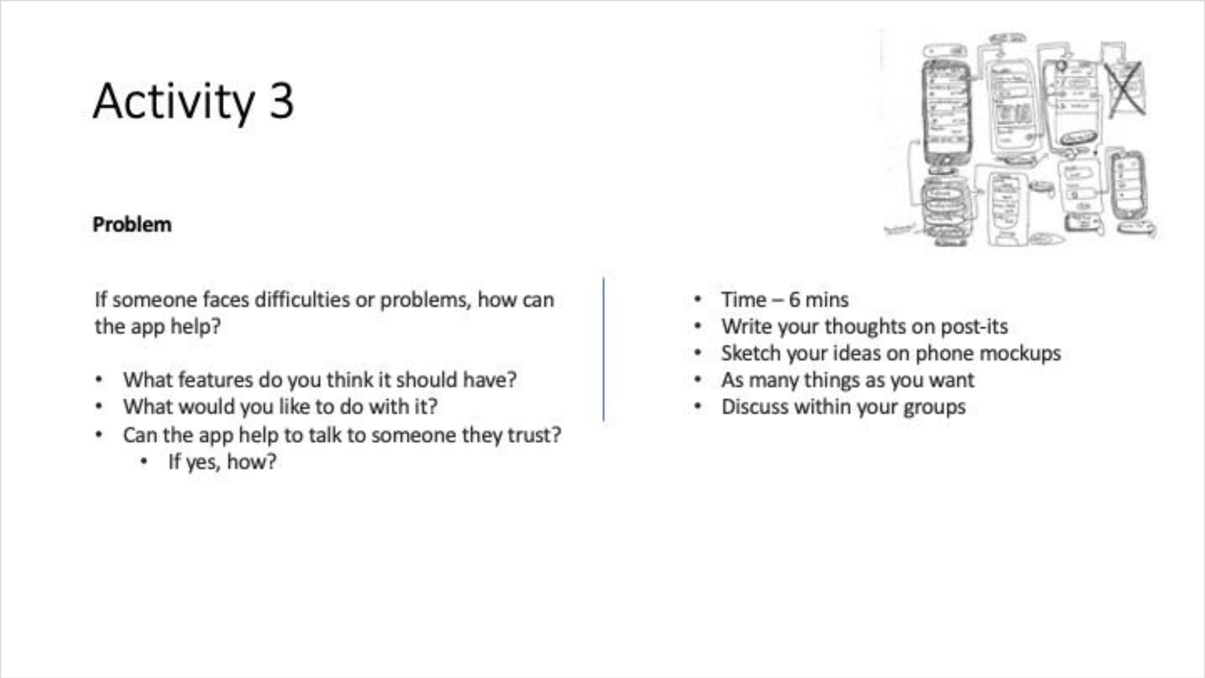
Tips

- Write an explanation
- Use simple elements; square, rounding, line, arrow, etc.
- Use realistic text
- Use a pen - it should be fast and does not have to be perfect
- If you make a mistake; just keep going
- If it goes completely wrong - curl up, throw away and take a new sheet



Tips for sketching screens: helpful patterns

Header
Tab
Filler text
User Picture
Photo
Video
Callouts
Can show alerts, help, guidance or sketch annotations
CALLOUT
Pop-up Module
POP-UP
Arrows
Larger ones can communicate weight, or act as labels
NEXT STEP
Drop Shadows
Communicate depth and bring attention to callouts or popup boxes
Calendar
Page curl
Mouse Cursor
Quietly indicates a rollover state
Side-scrolling Module



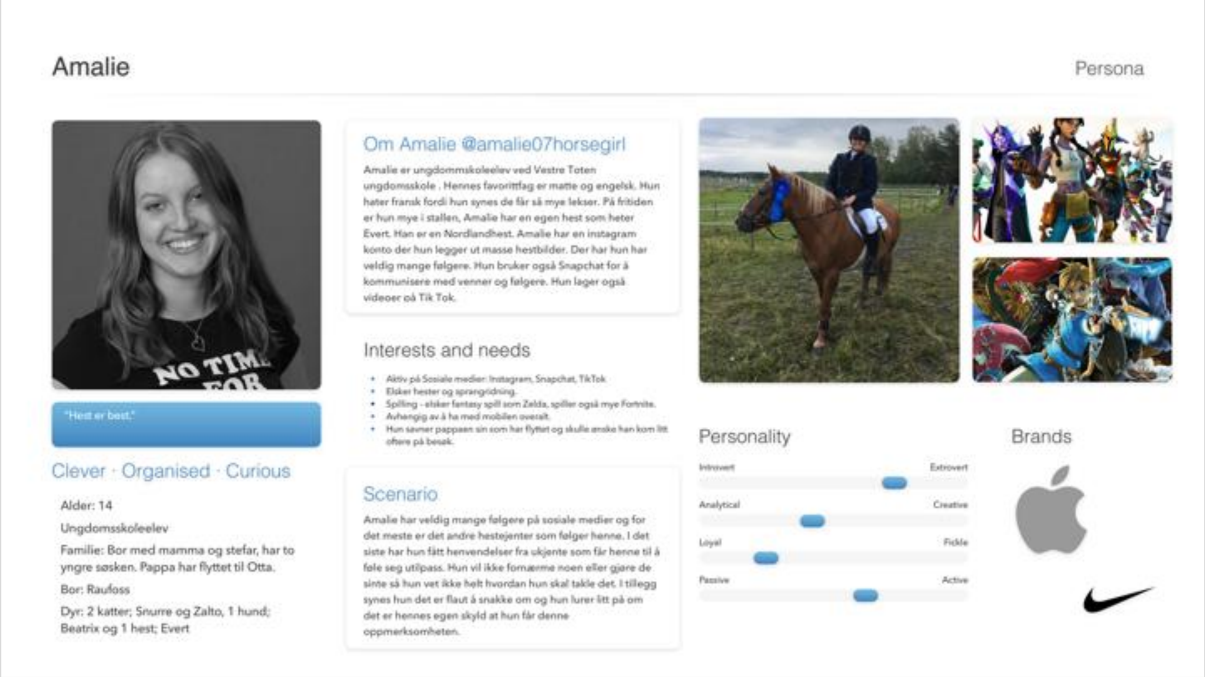
Activity 3

Problem

If someone faces difficulties or problems, how can the app help?

- What features do you think it should have?
- What would you like to do with it?
- Can the app help to talk to someone they trust?
    - If yes, how?

- Time – 6 mins
- Write your thoughts on post-its
- Sketch your ideas on phone mockups
- As many things as you want
- Discuss within your groups



Amalie

Persona

"Hest er best."

Clever · Organised · Curious

Alder: 14

Ungdomsskoleelev

Familie: Bor med mamma og stefar, har to yngre søsken. Pappa har flyttet til Otta.

Bor: Raufoss

Dyr: 2 katter; Snurre og Zalto, 1 hund; Beatrix og 1 hest; Evert

Om Amalie @amalie07horsegirl

Amalie er ungdommskoleelev ved Vestre Toten ungdomsskole . Hennes favorittfag er matte og engelsk. Hun hater fransk fordi hun synes de får så mye lekser. På fritiden er hun mye i stallen, Amalie har en egen hest som heter Evert. Han er en Nordlandhest. Amalie har en instagram konto der hun legger ut masse hestbilder. Der har hun har veldig mange følgere. Hun bruker også Snapchat for å kommunisere med venner og følgere. Hun lager også videoer oå Tik Tok.

Interests and needs

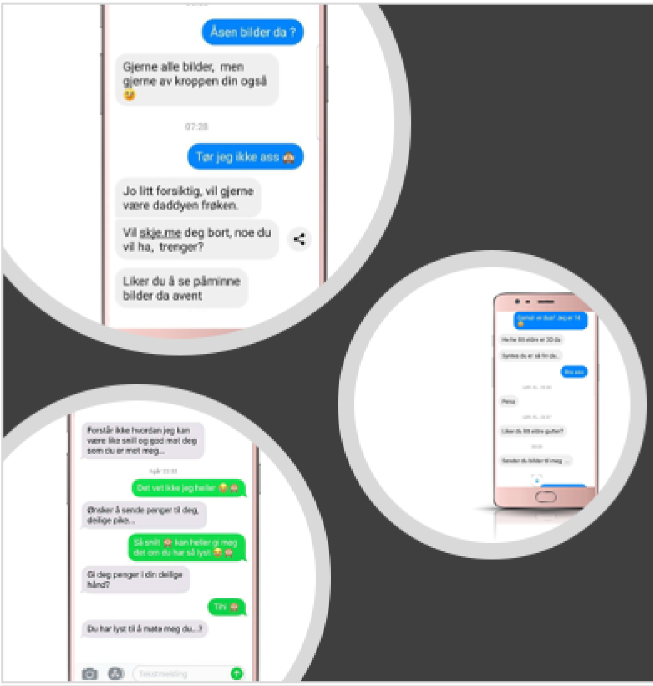
- Aktiv på Sosiale medier: Instagram, Snapchat, TikTok
- Elsker hester og sprangridning.
- Spilling - elsker fantasy spill som Zelda, spiller også mye Fortnite.
- Avhengig av å ha med mobilen overalt.
- Hun savner pappaen sin som har flyttet og skulle ønske han kom litt oftere på besøk.

Scenario

Amalie har veldig mange følgere på sosiale medier og for det meste er det andre hestejenter som følger henne. I det siste har hun fått henvendelser fra ukjente som får henne til å føle seg utilpass. Hun vil ikke fornærme noen eller gjøre de sinte så hun vet ikke helt hvordan hun skal takle det. I tillegg synes hun det er flaut å snakke om og hun lurer litt på om det er hennes egen skyld at hun får denne oppmerksomheten.

Personality

Brands



Åsen bilder da ?

Gjerne alle bilder, men gjerne av kroppen din også 😏

07:28

Tør jeg ikke ass 🙈

Jo litt forsiktig, vil gjerne være daddyen frøken.

Vil skje.me deg bort, noe du vil ha, trenger?

Liker du å se påminne bilder da avent

Gamle er du? Jeg er 14

Ha-ha litt eldre er 20 da

Synes du er så fin da..

Bra ass

Pena

Liker du litt eldre gutter?

Sender du bilder til meg ...

Forstår ikke hvordan jeg kan være like snill og god mot deg som du er mot meg...

Det vet ikke jeg heller 😇🙈

Ønsker å sende penger til deg, deilige pike...

Så snilt 🙈 kan heller gi meg det om du har så lyst 😇🙈

Gi deg penger i din deilige hånd?

Tihi 🙈

Du har lyst til å møte meg du...?

Tekstmelding

Amalie has a lot of followers on social media. Lately, she has received inquiries from unknown boys that make her feel uncomfortable.

She does not want to offend anyone or make them angry, so she does not quite know how to deal with it. In addition, she finds it embarrassing to talk about and she wonders a little if it is her own fault that she gets this attention.

Besides, she is afraid that her parents will take away her mobile if she says anything.

Activity 4

Problem

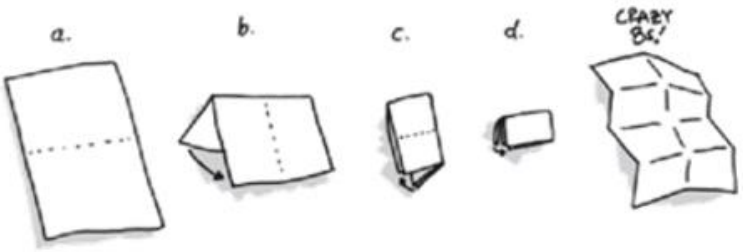
- Design an online feature that can help Amalie cope with this online grooming situation?
  - Group 1: Asking for Help (block, alert button, report to police..)
  - Group 2: Parental Notification
  - Group 3: Automated Assistance (identify fake profiles, flag suspicious behaviour)

- Crazy 8's – 10 minutes
- Pick 1 – spend 5 minutes on making it better
- Discuss within your groups

Crazy 8's

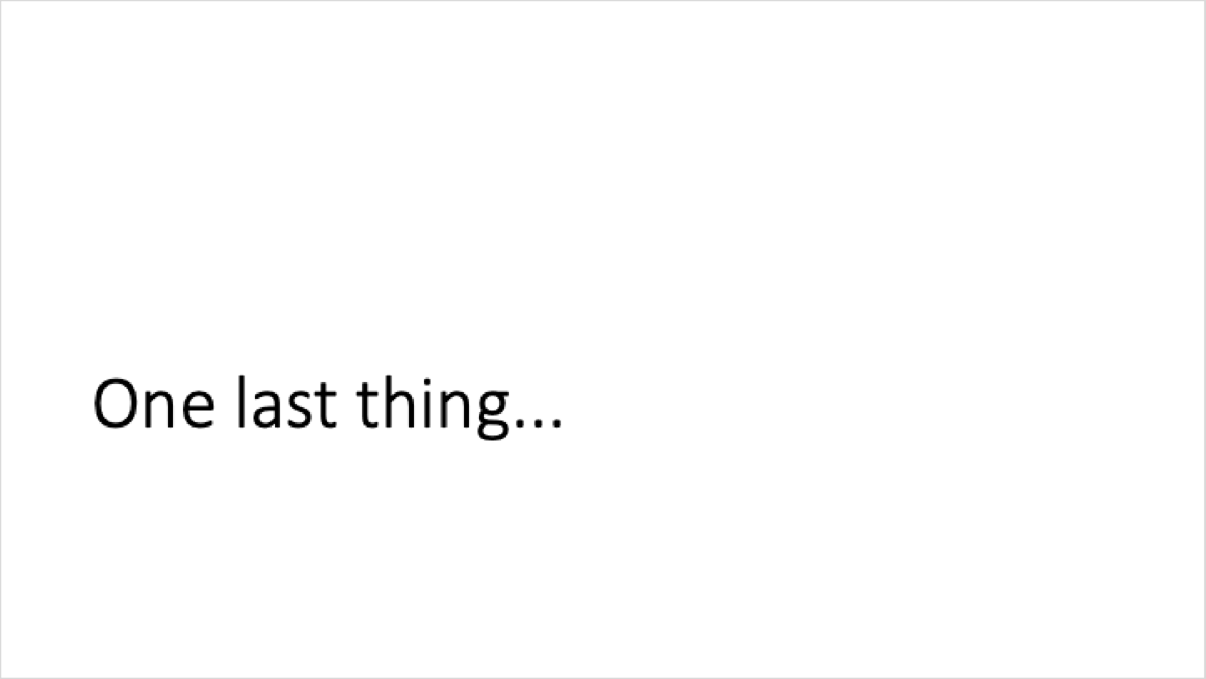
1. Brett et A4-ark i 8 (brett det på midten 3 ganger).
2. Tegn i ca **1 minutt** per rute (følg timer).

Tegn gjerne flere variasjoner av samme idé – bytt idé når du vil.

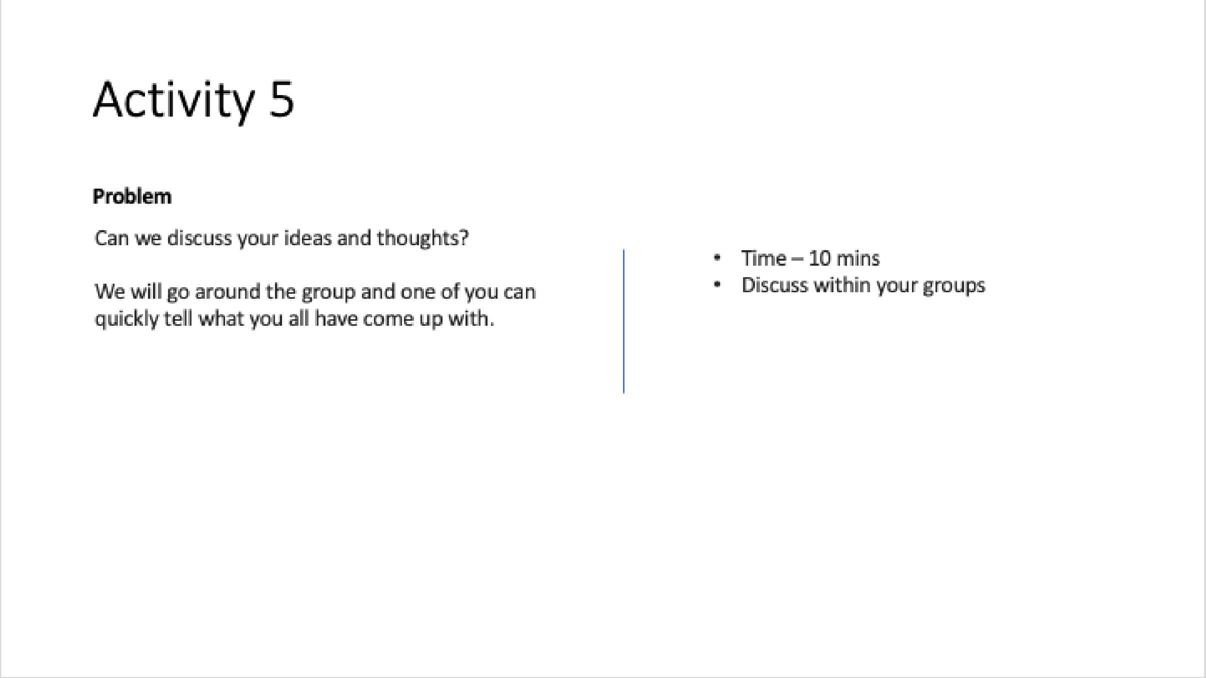


Velg 1 –

- Alle tegner sin beste idé på et ark.
- Løsningen skal være selvforklarende med tekst og piler.
- Ikke sett navn på.
- Stygt er bra (detaljert og fullstendig er viktig).



One last thing…



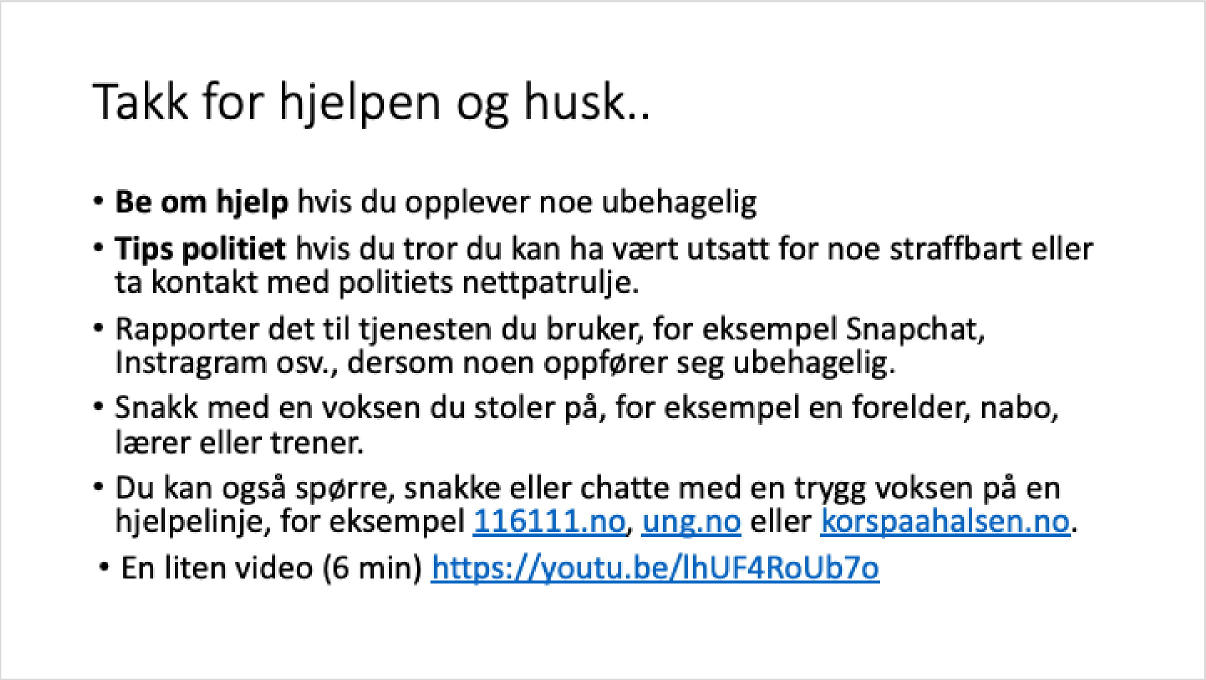
Activity 5

Problem

Can we discuss your ideas and thoughts?

We will go around the group and one of you can quickly tell what you all have come up with.

- Time – 10 mins
- Discuss within your groups



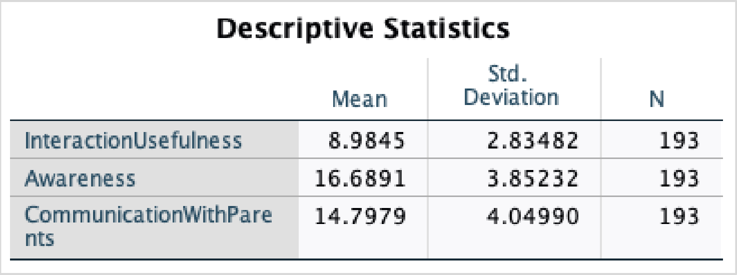
Takk for hjelpen og husk..

- **Be om hjelp** hvis du opplever noe ubehagelig
- **Tips politiet** hvis du tror du kan ha vært utsatt for noe straffbart eller ta kontakt med politiets nettpatrulje.
- Rapporter det til tjenesten du bruker, for eksempel Snapchat, Instragram osv., dersom noen oppfører seg ubehagelig.
- Snakk med en voksen du stoler på, for eksempel en forelder, nabo, lærer eller trener.
- Du kan også spørre, snakke eller chatte med en trygg voksen på en hjelpelinje, for eksempel 116111.no, ung.no eller korspaahalsen.no.
- En liten video (6 min) https://youtu.be/lhUF4RoUb7o

8.6 Survey results

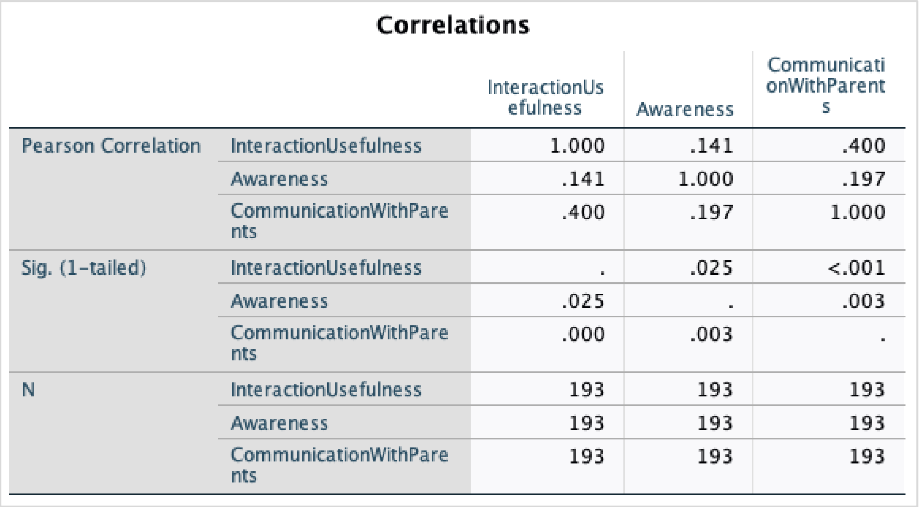
8.6.1 Regression analysis

Detailed regression test results of Awareness (independent variable), CommunicationWithParents (independent variable) and InteractionUsefulness (dependent variable) are as follows.



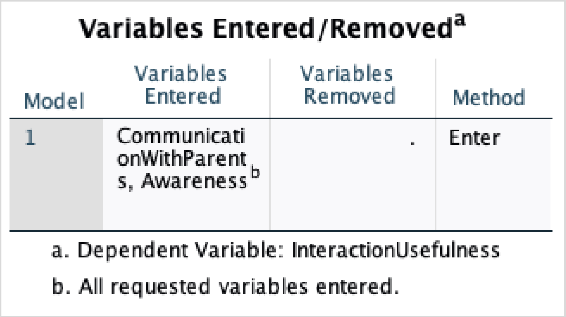
Descriptive Statistics

	Mean	Std. Deviation	N
InteractionUsefulness	8.9845	2.83482	193
Awareness	16.6891	3.85232	193
CommunicationWithParents	14.7979	4.04990	193



Correlations

		InteractionUsefulness	Awareness	CommunicationWithParents
Pearson Correlation	InteractionUsefulness	1.000	.141	.400
	Awareness	.141	1.000	.197
	CommunicationWithParents	.400	.197	1.000
Sig. (1-tailed)	InteractionUsefulness	.	.025	<.001
	Awareness	.025	.	.003
	CommunicationWithParents	.000	.003	.
N	InteractionUsefulness	193	193	193
	Awareness	193	193	193
	CommunicationWithParents	193	193	193

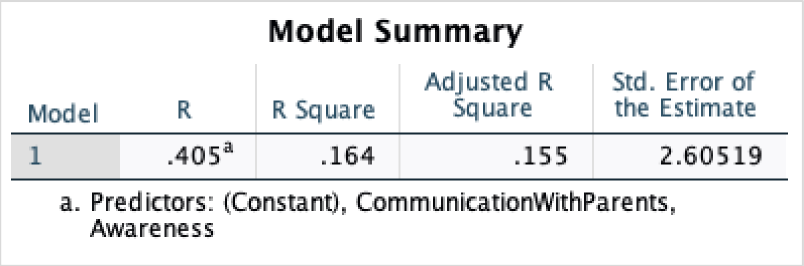


Variables Entered/Removed[a]

Model	Variables Entered	Variables Removed	Method
1	CommunicationWithParents, Awareness[b]	.	Enter

a. Dependent Variable: InteractionUsefulness

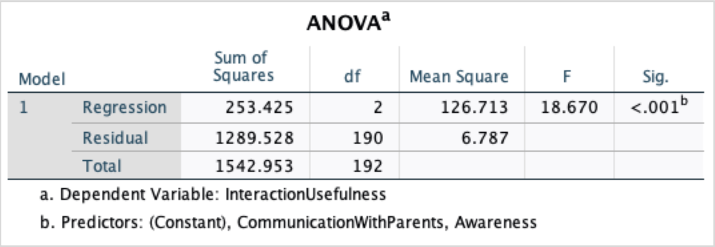
b. All requested variables entered.



Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.405[a]	.164	.155	2.60519

a. Predictors: (Constant), CommunicationWithParents, Awareness

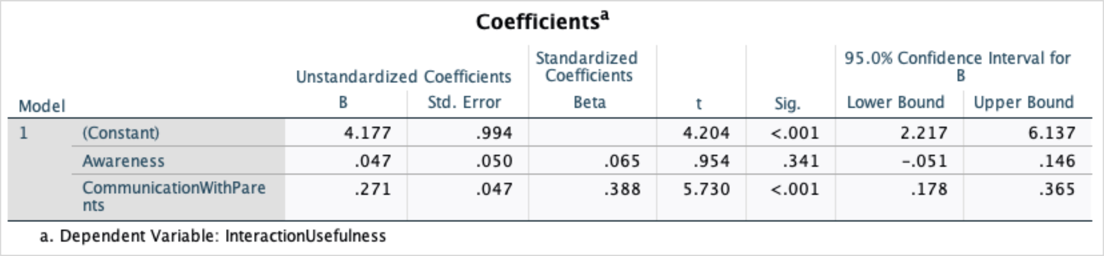


ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	253.425	2	126.713	18.670	<.001[b]
	Residual	1289.528	190	6.787		
	Total	1542.953	192			

a. Dependent Variable: InteractionUsefulness

b. Predictors: (Constant), CommunicationWithParents, Awareness

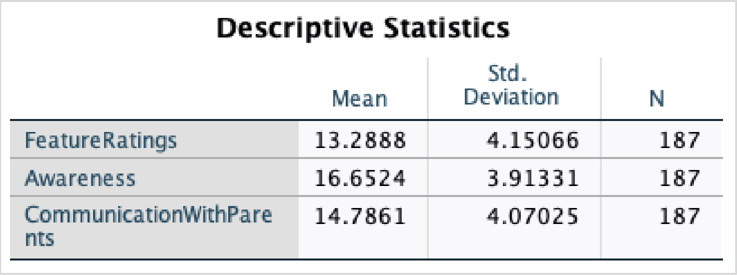


Coefficients[a]

		Unstandardized Coefficients		Standardized Coefficients			95.0% Confidence Interval for B	
Model		B	Std. Error	Beta	t	Sig.	Lower Bound	Upper Bound
1	(Constant)	4.177	.994		4.204	<.001	2.217	6.137
	Awareness	.047	.050	.065	.954	.341	-.051	.146
	CommunicationWithParents	.271	.047	.388	5.730	<.001	.178	.365

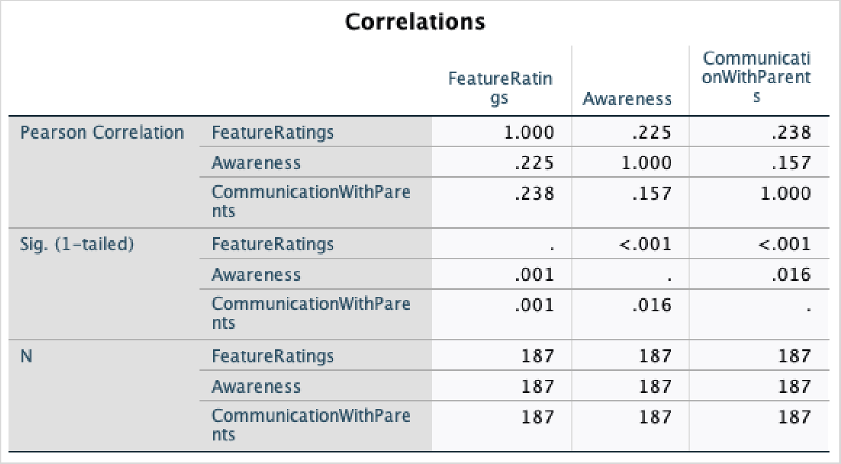
a. Dependent Variable: InteractionUsefulness

Detailed regression test results of Awareness (independent variable), CommunicationWithParents (independent variable) and FeatureRatings (dependent variable) are as follows.



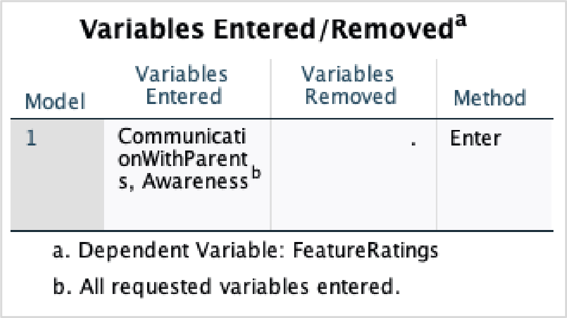
Descriptive Statistics

	Mean	Std. Deviation	N
FeatureRatings	13.2888	4.15066	187
Awareness	16.6524	3.91331	187
CommunicationWithParents	14.7861	4.07025	187



Correlations

		FeatureRatings	Awareness	CommunicationWithParents
Pearson Correlation	FeatureRatings	1.000	.225	.238
	Awareness	.225	1.000	.157
	CommunicationWithParents	.238	.157	1.000
Sig. (1-tailed)	FeatureRatings	.	<.001	<.001
	Awareness	.001	.	.016
	CommunicationWithParents	.001	.016	.
N	FeatureRatings	187	187	187
	Awareness	187	187	187
	CommunicationWithParents	187	187	187

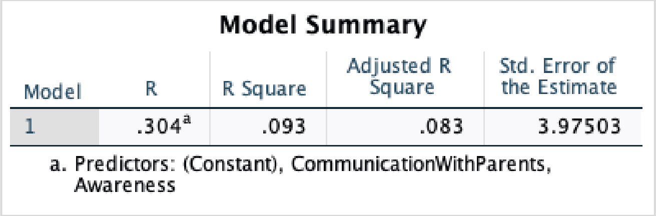


Variables Entered/Removed[a]

Model	Variables Entered	Variables Removed	Method
1	CommunicationWithParents, Awareness[b]	.	Enter

a. Dependent Variable: FeatureRatings

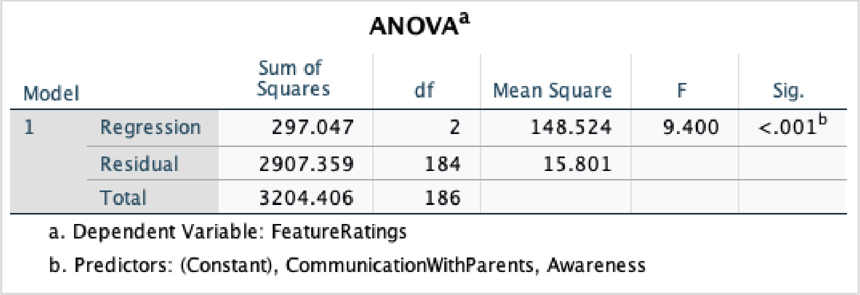
b. All requested variables entered.



Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.304[a]	.093	.083	3.97503

a. Predictors: (Constant), CommunicationWithParents, Awareness

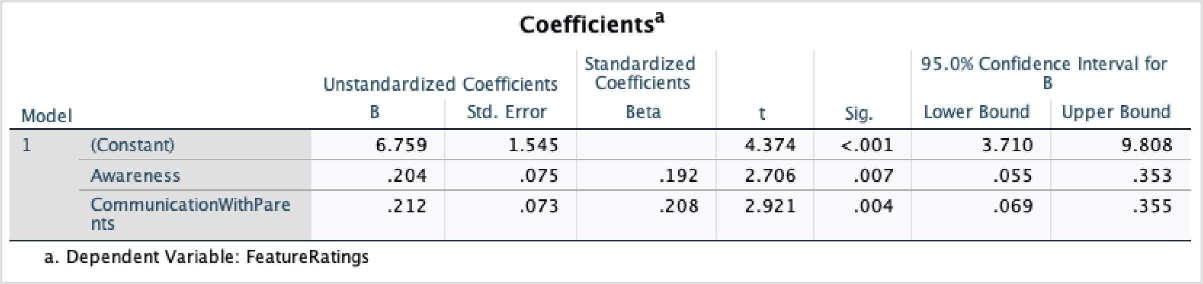


ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	297.047	2	148.524	9.400	<.001[b]
	Residual	2907.359	184	15.801		
	Total	3204.406	186			

a. Dependent Variable: FeatureRatings

b. Predictors: (Constant), CommunicationWithParents, Awareness



Coefficients[a]

		Unstandardized Coefficients		Standardized Coefficients			95.0% Confidence Interval for B	
Model		B	Std. Error	Beta	t	Sig.	Lower Bound	Upper Bound
1	(Constant)	6.759	1.545		4.374	<.001	3.710	9.808
	Awareness	.204	.075	.192	2.706	.007	.055	.353
	CommunicationWithParents	.212	.073	.208	2.921	.004	.069	.355

a. Dependent Variable: FeatureRatings

8.7 Interactive prototype

The interactive prototype can be viewed at this link. Alternatively, the following link can be copy pasted in a latest browser –

https://www.figma.com/proto/BHH6hKZsQYD17mJcMgkxzK/AiBA-Prototype?page-id=0%3A1&node-id=1%3A3&viewport=-1128%2C275%2C0.4812253415584564&scaling=scale-down

The prototype shows different interactive elements. Interactive elements can be viewed by clicking anywhere on the page, a blue highlight around the interactive elements will appear. The prototype is best viewed in full screen mode, accessible from top right corner.

Nakul Pathak

Building Effective Interactions

NTNU
Norwegian University of
Science and Technology