My Data or Our Data? A Comparative Study of Collaborative Family Apps and Parents' Experiences with Apple's Family Sharing

Amel Bourdoucen
Aalto University
Finland
amel.bourdoucen[at]aalto.fi

Janne Lindqvist
Aalto University
Finland
janne.lindqvist[at]aalto.fi

Abstract

Collaborative family apps are designed for families to stay connected, look after their kids, and share life events. Despite their well-intended design, collaborative family apps can be invasive, leading to tensions in family relationships and exposure to online risks. We compared frequently downloaded collaborative family and parental control apps in terms of their features, with a focus on Apple's Family Sharing and Google's Family Link. We then conducted a qualitative interview study (N=20) to explore privacy experiences when using Apple's Family Sharing. Our results highlight privacy challenges with the use of collaborative family apps to negotiate boundaries and manage content, such as mismanaging finances and accidental content sharing. We reveal that roles and hierarchies on the app are unclear, leading to users' confusion about the privacy controls associated with each role. Based on these insights, we propose design recommendations to address these challenges and enhance the usability and privacy of collaborative family apps.

Keywords

parents, families, children, parental apps, collaborative family apps, privacy, mobile devices

1 Introduction

Parents are concerned about the online safety of their children and their screen time. According to a recent study in 2023 [50], following the COVID-19 pandemic, the average screen time for children increased by 1.4 hours, bringing them to an average of four hours per day on their mobile devices. Excessive screen time in early childhood can lead to developmental issues [2, 73, 97], physical health problems—obesity, poor sleep, and eyestrain—[73] and reduced attention span [97]. Children are also exposed to many online risks, such as inappropriate content, cyberbullying, online predators, privacy breaches, and data exploitation [40, 62, 100]. A recent study found that 42% of children aged 10–17 have accidentally ended up on inappropriate websites, with the average age of first exposure being 9 years old [88].

To address these issues, parents resort to parental control apps to protect their children from various online risks and monitor their screen time. Parental apps allow parents to block content, manage screen time, and track locations. Popular examples of parental apps are *Qustodio* and *Norton Family* . While these apps provide a sense of safety, they may also negatively impact children's sense of autonomy and trustworthiness [94], creating tensions [5, 47]. Research suggests that parental control apps can be invasive and overly restrictive of children's and teens' online privacy [46, 64]. Researchers have suggested more collaborative solutions for parents and teens to work to make safety decisions together [46].

Collaborative family apps take a different approach with *coactive* sharing information and managing tasks collectively as a family. Popular examples of collaborative family apps are Apple's Family Sharing and Google's Family Link, though they vary; see Figure 1. Collaborative family apps may help counteract the negative effects of parental control apps. Yet, there is limited research on collaborative family apps beyond the traditional focus on parental monitoring of children. In the present study, we investigate how parents use Apple's Family Sharing app—one example of a collaborative app—to serve their needs and what their understanding of their privacy on the app is.

As of 2024, Apple's market share is extensive, with over 1 billion users worldwide using at least one Apple device [16, 65]. Moreover, according to a recent survey [99], 60% of Apple users in the U.S. own more than one Apple device. Owning multiple Apple devices within a family allows families to share purchases such as apps, music, movies, and subscriptions without sharing accounts or passwords.

In this study, we examine how well users understand and utilize privacy controls in shared contexts, exploring the extent to which they can effectively maintain their sense of privacy while benefiting from the convenience of shared devices.

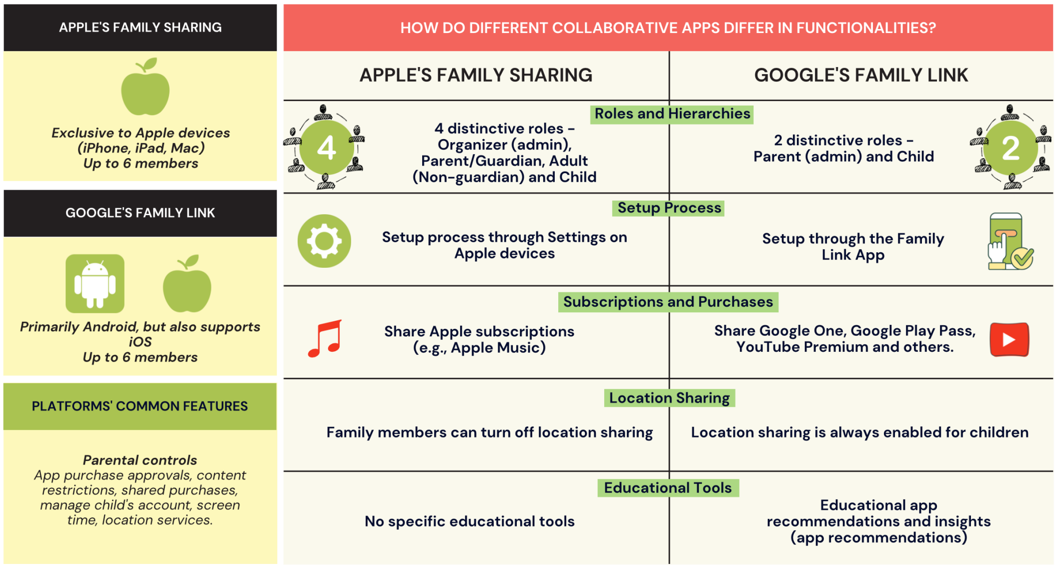
We investigate three research questions:

(1) **RQ1:** How do families translate their needs through collaborative family apps?
(2) **RQ2:** How do family members understand the privacy settings of collaborative family apps?
(3) **RQ3:** What are the impacts that collaborative family apps have on family relationships?

To answer these research questions, we first selected the 13 most popular parental and collaborative family apps on app stores. We compared the apps for their features to determine the personal data collected from families when using the apps. We focused on Apple's Family Sharing and Google's Family Link for an in-depth comparison. Based on this, we then conducted a user study (N=20) with a focus on users of Apple's Family Sharing app. The study examined how the app assisted families in day-to-day activities

Proceedings on Privacy Enhancing Technologies 2025(4), 812–837

https://doi.org/10.56553/popets-2025-0159



APPLE'S FAMILY SHARING

Exclusive to Apple devices (iPhone, iPad, Mac) Up to 6 members

GOOGLE'S FAMILY LINK

Primarily Android, but also supports iOS Up to 6 members

PLATFORMS' COMMON FEATURES

Parental controls
App purchase approvals, content restrictions, shared purchases, manage child's account, screen time, location services.

HOW DO DIFFERENT COLLABORATIVE APPS DIFFER IN FUNCTIONALITIES?

	APPLE'S FAMILY SHARING	GOOGLE'S FAMILY LINK
Roles and Hierarchies	4 distinctive roles – Organizer (admin), Parent/Guardian, Adult (Non-guardian) and Child	2 distinctive roles – Parent (admin) and Child
Setup Process	Setup process through Settings on Apple devices	Setup through the Family Link App
Subscriptions and Purchases	Share Apple subscriptions (e.g., Apple Music)	Share Google One, Google Play Pass, YouTube Premium and others.
Location Sharing	Family members can turn off location sharing	Location sharing is always enabled for children
Educational Tools	No specific educational tools	Educational app recommendations and insights (app recommendations)

Figure 1: An overview of the key differences and similarities between Apple's Family Sharing and Google's Family Link. While both apps incorporate many collaborative features, they differ slightly in some areas such as the setup process and roles and hierarchies on the app. Apple's Family Sharing is also exclusive to Apple's devices while Google's Family Link is available primarily on Android but also on iOS. Both apps are very similar in the parental control tools they provide, such as app purchase approvals, content restrictions, shared purchases, and managing a child's account.

and the possible impacts the app had on parents and their families when sharing personal data.

We found that many parents used parental control apps before shifting to collaborative family apps. When using collaborative family apps, parents highlighted privacy challenges due to sharing content accidentally. In particular, this was when the content shared was considered personal by the family member. In similar cases, parents shared that they experienced the app having an impact on their family relationships, either between partners or between parents and children. Some of the privacy concerns expressed by parents stemmed from a lack of information on how to control their privacy settings on the app. We discuss how users understand their privacy on the app and use the apps to serve their needs as a family. We explore the implications that may occur when using the app to share as a family.

We summarize our main contributions as follows:

(1) We provide an in-depth comparative analysis of popular collaborative family apps and an examination of their functionalities, with a focus on Apple's Family Sharing and Google's Family Link. We highlight the key differences and similarities between collaborative family apps and the privacy controls of the roles on the app, (2) we reveal concerns and challenges in collaborative family apps to negotiate boundaries and manage content, and highlight potential harmful implications that can affect parents and children using the app, (3) we provide recommendations and design implications for app developers and researchers that reflect family needs through collaborative family apps.

2 Background and Related Work

Parents use a variety of online apps designed to help protect and monitor their children's behavior online. The large number of emerging social media apps and media content has made the use of such apps needed. People spend much more of their time online, as a recent large-scale study in 2021 [81] with 11,875 children suggested a relationship between screen time and the amount of sleep and academic performance in children. This can be concerning to parents, and it can motivate them to adopt different solutions to restrict their children's use of their phones. Parents are motivated to adopt technology primarily to protect their children from online risks like adult content, predators, and cyberbullying [45, 90], and to maintain visibility over their activities [107]. For example, GPS tracking is a common feature, and children aged 10–14 have reported receiving mobile devices partly for this purpose [59]. However, while parents seek control, teens may use the same technology to assert independence [64].

2.1 Theoretical Perspectives on Family Privacy and Technology Use

We explore theories that examine the interplay between user privacy and technology adoption to translate individual needs and family needs when using technologies.

Contextual Integrity (CI), proposed by Nissenbaum [75, 76], frames privacy as the appropriate flow of personal information within specific social contexts, where expectations depend on roles, norms, and transmission principles. A violation occurs not when information is merely shared, but when it is shared in a manner that conflicts with contextual expectations. Contextual Integrity has been applied to different contexts, such as AI tools [53, 71, 87], social media [6], and smart home personal assistants [1].

Privacy Calculus theory [60] explains how users make disclosure decisions by weighing the perceived benefits of sharing against the potential risks. Later work—especially in information systems and HCI—expanded this theory to digital contexts (e.g., mobile apps [58, 103], social media [98], smart devices [91], AI chatbots [69]).

Interdependent Privacy (IDP) [21] highlights that privacy is not only shaped by individual decisions but also by the behaviors and preferences of others in a shared system. IDP has been applied to different contexts, like smart homes [7], social platforms [39], co-location [79], and even genomic data sharing [20], where one user's actions can inadvertently expose others. However, an underexplored dimension of IDP is restricted self-disclosure, that is, situations where one user prevents another from sharing their own information. Together, these theoretical perspectives demonstrate that privacy in family settings is inherently relational, contextual, and role-dependent. The current work builds on and extends this body of research by highlighting how collaborative family apps not only mediate interpersonal data sharing but also facilitate control over others' ability to manage their own data, a less examined yet critical aspect of privacy in domestic technology use.

2.2 Challenges and Risks in the Use of Parental Control Apps

2.2.1 Children and Teens. Research has explored the use of parental control apps to monitor children and the effect of that on family relationships. Parents rely on control apps to monitor their children's behavior online.

Parental control apps can feel overly restrictive—imposing excessive limitations that interfere with everyday use of devices and create feelings of frustration or oppression—which may lead children to rebel against parental authority [46]. In a recent study by Feal et al. [37] on 46 apps with a combined 20M downloads, it was suggested that parental control applications often pose privacy risks for children [37]. Another study showed that teens who were victimized online were likely monitored by their parents [47]. The likelihood of children being exposed to security threats is common from a family member or friend [108]. Research has also explored the concept of *sharenting* and the normalization of parental monitoring of children as a necessary aspect of child care [63]. One potential risk identified is that surveillance of children may give the message to children that they are not to be trusted [94].

Studies proposed that technology can be invasive to the privacy of children [46] and can create tensions in relationships [32, 46, 59]. A study by Ghosh et al. [46] analyzed 37 mobile online safety apps from Google Play and suggested that 14% of these supported bad parenting and a lack of communication, while 35% of the apps were overly restrictive for children [5, 46]. Children expressed resentment when being monitored through their mobile devices [46, 47], creating tensions in parent-child relationships [5, 47].

Research shows that parental rules often target screen time rather than usage context [52, 59], while children seek privacy from parents, such as by keeping social media accounts hidden [30, 59]. Some studies suggest involving children more in parenting decisions [49].

2.2.2 Adults. Research on the use of apps for sharing information between adults showed that collaborative use of technology can have a positive impact on relationships, fostering stronger connections and promoting joint decision-making. Sharing information can improve transparency and trust [9]. Collaboration on shared tasks promotes teamwork and mutual support [24]. Sharing information positively impacts relationship development [95].

Past research underscores how mobile phones and social media apps can be exploited in relationships for harmful activities like harassing, stalking, and revenge pornography [41, 42, 68]. Stalking often involves the installation of spyware on the victim's devices, typically by an intimate partner, allowing invasive tracking of the victim's movements and communications [27]. Common stalking tactics also include persistent, unwanted calls and messages [22].

Digital devices and online accounts are frequently shared within close relationships (e.g., households, couples, siblings), and current technology designs—often based on a single-user model—fail to reflect the complexity, context, and relational nature of this sharing. Matthews et al. [67] show that device and account sharing is routine in households, including mobile phones, which are usually assumed to be personal. They identify different types of sharing and highlight motivations like trust and convenience. Jacobs et al. [56] focus on couples and how they navigate access, often unintentionally or without clear boundaries. They reveal the importance of relationship context in determining what sharing is appropriate. In cross-cultural sharing, sharing can be expected and normalized, but not necessarily safe or private. Al-Ameen et al. emphasize that privacy expectations are shaped by culture and access norms [4]. Sambasivan et al. [89] examine how women in low-income South Asian households navigate privacy on shared mobile devices. Women often use phones controlled by male relatives, leading to surveillance and restricted digital autonomy. To cope, women adopt subtle strategies like deleting messages or using innocuous apps, a practice the authors term "performative privacy" [89]. Therefore, privacy may not be treated as a static, individualistic right but rather a dynamic, negotiated process shaped by family, gender roles, and collective norms.

In summary, prior work discussed the consequences of children using parental control apps: children expressing resentment [46, 47], children hiding aspects of their online experience from their parents [59], tensions in parent-child relationships [5, 47], and privacy risks that children are exposed to even with the use of these supposedly protective apps [37]. Prior work also highlighted exposure of intimate partners and how technology is used as a medium to facilitate such actions [22, 27, 66].

While previous research has explored the effects of monitoring on parent-child and interpersonal relationships, it has largely focused on parental control apps that reinforce hierarchical dynamics within families. Importantly, these studies have not delved into how such apps impact the privacy of adults who use them, such as co-parents or other guardians. Our work is the first to investigate whether collaborative family apps offer a more effective way to help families safely navigate online spaces. This study identifies key challenges affecting both collaborative family apps and parental control apps, providing insights that can guide future designs to better serve the needs of all family members, including adults.

3 Study I: Comparing Apps

In this study, we examine, compare, and summarize the features and functionalities of 13 apps designed for family use, with a particular focus on Apple's Family Sharing and Google's Family Link. These two platforms were chosen as focal points due to their popularity and their representation of the iOS and Android ecosystems, respectively. Google's Family Link, in particular, was selected as a robust counterpart to Apple's Family Sharing because it is widely used and operates within the Android ecosystem.

3.1 Method of Study 1

We began by analyzing top-rated apps from the Google Play Store and Apple App Store, as ranked by the stores' algorithms based on user ratings and relevance to search queries [15]. The apps are compared according to the features that they offer and the platforms they are available on. We updated our app list in 2025, building on our original dataset collected in 2022. To ensure continued relevance, we reviewed the top apps in both the App Store and Google Play Store using keywords such as 'parental control' and 'family apps'. Apps were included if they had over 100,000 downloads, a rating above 4.0, and offered at least two relevant features. As a result, seven new apps were added, and the remaining apps from the original 2022 list were confirmed to still be relevant.

The final list of apps were: Apple's Family Sharing [14], Google Family Link [48], Aura Parental Control [18], Bark Premium [19], Kaspersky Safe Kids [57], Qustodio [85], Net Nanny [74], Norton Family [77], OurPact [80], FamiSafe [104], Mobicip [70], Canopy [25], and MMGuardian [82].

We employed a feature comparison approach, a commonly used method in HCI and usability research, to systematically analyze the functionalities and limitations of related technologies (e.g., [23, 43, 86, 96]). Feature comparison has been widely utilized in usability evaluations and security studies to identify gaps and opportunities for design improvements.

To ensure a systematic comparison, we followed a structured process: (1) identifying key features based on prior literature and system documentation, (2) defining criteria for the comparison, (3) independently reviewing and validating features, and (4) resolving discrepancies through discussion. The feature selection and classification were reviewed by the group of researchers, and disagreements were addressed through iterative refinement, for the sake of consistency.

Our goal was to identify the key differences in how traditional parental control apps operate versus collaborative models by evaluating the range of features provided by each. Our investigation revealed significant differences between collaborative family apps and traditional parental control apps. Traditional parental control apps typically adopt a *hierarchical structure*, where one user—often a parent—exerts unilateral control over another's device or activity, such as setting screen time limits or content restrictions without reciprocal access. In contrast, collaborative family apps, like Apple's Family Sharing, incorporate other features apart from what parental app controls provide, such as mutual visibility and shared responsibility, including shared calendars, purchases, and location. We focused on Apple's Family Sharing and Google's Family Link, both collaborative family apps, and analyzed their features in depth, as they provided more features than traditional parental control apps in Table 1.

To thoroughly compare and analyze the functionalities and privacy options for every app, we examined the following sources and documents using content analysis [35]: (1) The apps' official webpages and download sources, for the functions of each app; (2) the privacy policies of Apple's Family Sharing app and Google's, for information about data-handling processes; and (3) Apple's and Google's support pages, for an initial understanding of the configuration of different features. Content analysis allowed us to extract relevant information about the presence of features such as location tracking, screen time limits, media sharing, cloud space, apps and subscriptions, and content filters, as well as the associated privileges granted to different user roles (e.g., Organizer, Parent/Guardian, Child). In addition to analyzing these documents, we conducted cognitive walkthroughs of the apps to explore and evaluate their features in practice. This step was performed exclusively by expert researchers without user participation.

3.2 Results of Study 1

We provide a comparison of different parental and collaborative family apps, noting their main features, in Table 1 in Appendix 8.4: location tracking, screen time allocation, media sharing, cloud space, apps and subscriptions, and content filters.

Our analysis also serves the purpose of highlighting the difference between traditional parenting apps and collaborative family apps. In this table, we observe through our analysis of app features that traditional parental apps have in common that they mainly provide monitoring features for child protection. The exceptions to this are Apple's Family Sharing and Google's Family Link, which allow members to share cloud storage plans and family photos and locate each other's missing devices [14]. For example, Apple's Family Sharing allows for customization of content so that each family member can maintain their access to subscriptions and storage space even in a family context.

To prepare content for the second study, we needed to conduct background analysis of Apple's Family Sharing. Apple's Family Sharing stands out as a uniquely comprehensive solution within a closed ecosystem, offering content customization, purchase sharing, location tracking, and subscription management within a unified platform. This level of integration and control over digital family interactions makes Apple's Family Sharing a compelling case study for understanding the privacy and usability challenges of collaborative family apps. While Google's Family Link shares some similar features, its focus remains more on parental control, making Family Sharing an ideal choice for an in-depth exploration of collaborative digital parenting.

Due to the closed nature of Apple's ecosystem, however, such analysis could only be done on the documents distributed officially by Apple [23]. We analyzed the official documents provided by Apple on how to use Apple's Family Sharing, and we looked at the following features of Apple's Family Sharing: Location Sharing (GPS locator), Ask to Buy, Screen Time, Purchase Sharing, iCloud+ (Cloud Space), Apple Subscriptions and App Store Subscriptions [12]. The initial study was carried out in 2022. However, with the release of recent operating systems in 2024, we have updated Study

Table 1: Analysis of parental control apps and family apps and their features. (*) Google Family Link doesn't natively include direct media-sharing features like Apple's Family Sharing. However, you can still share media with Family Link by leveraging other Google services that integrate with the Family Link ecosystem, such as Google Drive (cloud space) and Google Photos (media).

Apps	*Type*	Location tracking	Screen time limits	Media	Cloud Space	Apps and Subscriptions	Content filters
Apple Family Sharing	Collaborative	x	x	x	x	x	x
Google Family Link	Collaborative	x	x	x*	x*	x	x
Aura Parental Control	Parental Control	x	x				x
Bark Premium	Parental Control	x	x				x
Kaspersky Safe Kids	Parental Control	x	x				x
Qustodio	Parental Control	x	x				x
Net Nanny	Parental Control	x	x				x
Norton Family	Parental Control	x	x				x
OurPact	Parental Control	x	x				x
FamiSafe	Parental Control	x	x				x
Mobicip	Parental Control	x	x				x
Canopy	Parental Control	x	x				x
MMGuardian	Parental Control	x	x				x

I to reflect the latest version of Apple's Family Sharing app and Google's Family Link to provide a contrast between these two family solutions provided on iOS and Android, respectively.

3.2.1 *Apple's Family Sharing.*

The following are the main observations of the functionality of the features of Apple's Family Sharing, as well as their privacy configurations. This work includes annotated screenshots of the app interface as supplementary materials [8].

(1) *Roles in Apple's Family Sharing:* Roles in Family Sharing assist in organizing privileges. The roles are defined as the following: (i) *Organizer (admin):* the main admin who sets up the family group and manages members, roles, purchases, and sharing settings. (ii) *The Parent/Guardian:* an adult who can manage child settings like screen time and purchase approvals but cannot change family roles. (iii) *Adult:* a regular family member who can access shared content but cannot manage other members or settings. (iv) *Child:* a minor with restricted permissions who needs adult approval for purchases and has limited control over their account. Children below the age of 13 cannot create Apple IDs on their own (this varies by region) [11]. A summary of the roles, privileges, and hierarchies is found in Table 2.

(2) *Location tracking:* Family members can keep track of each other's locations. Apple's Family Sharing allows family members to decide if they want to share their location or not. Family members can assist each other to find their lost devices. Family members can check the device's online/offline status, play a sound, or completely erase the device [10].

(3) *Sharing content with family members:* Family Members can also share apps and purchases from the iTunes Store, App Store, Apple Books, and Apple TV Purchases [13].

(4) *Controlling privacy on the app:* If a family member decides to leave the family—that is, no longer use the Apple's Family Sharing app—certain things will change. The member's Apple ID will be removed from the family group and they will no longer have access to the items shared by the family. It is important to note that a child cannot quit a family the same way adults can. Other personal information that will stop being shared with other family members include location, previous purchases, photo albums, and calendars.

Variances in the interface in the app between 2022 and 2024: There were small updates in the interface since the study was conducted in 2022 e.g., more tips for users. A tip under the family usernames indicates more information about what happens when you add features like adding a family member to an emergency contact, sharing location, or adding a recovery contact or legacy contact.

3.2.2 *Google's Family Link.*

In Google's Family Link, there are two primary roles: Parent and Child. The roles and privileges in Google's Family Link are summarized in Table 3. The privacy configurations available to children are primarily controlled by their parents. This means that when parents grant children permission, many settings are available for them to manage, such as controls that affect what data is saved to their Google account. These settings include: Web & App Activity, Location History, and YouTube History.

Children may have restricted or a "limited" degree or control or access to these features (see the list of features in Table 3).

With the app, Parents can: (1) *Manage apps:* approve or block apps that children can download from the Google Play Store. (2) *Manage screen time:* set daily usage limits to help manage screen time. (3) *Set content filters:* enable SafeSearch to filter explicit content. (4) Set *location tracking*. (5) *Manage contacts:* on Google Hangouts or Messages.

Children can control some aspects of these features in the app, but more comprehensive privacy settings related to these features are controlled by the Parent:

(1) *View and manage Google activity controls:* children may be able to view web searches and location history, but they cannot turn off these controls without their parents' permission. (2) *Modify personal information:* children can view their personal information, such as name or profile picture, but changes to important details such as

Table 2: The table illustrates the different privileges of roles in Apple's Family Sharing. The *Organizer* represents the administrator in this setting. Only the family *Organizer* can set up purchase sharing, assigning roles to members and adding members to the family. The *Organizer* and the *Parent/Guardian* can both approve *Child*-related settings (for instance, approving purchases and downloads for a *Child*).

Features	*Child*	*Adult*	*Parent/Guardian*	*Organizer*
Can create a family				x
Can delete a family				x
Can assign roles				x
Can add members				x
Create Child Account			x	x
Enable Ask to Buy for child			x	x
Manage screen time settings			x	x
Approve Ask to Buy requests			x	x
Approve Downloads			x	x
Approve Purchases			x	x
Approve Apple Books			x	x
Approve iTunes			x	x
Stop Using Family Sharing		x	x	x
Setup Purchase Sharing				x
Setup iCloud+		x	x	x
Access to Location Sharing	x	x	x	x
Access to Ask to Buy	x			
Access to Screen Time	x			
Access to Apple Subscriptions	x	x	x	x
Access to App Store Subscriptions	x	x	x	x
Access to iCloud+	x	x	x	x

Table 3: The table illustrates the different privileges of roles in Google's Family Link. The *Parent/Guardian* role represents the administrator in this setting, who is capable of managing the device and account settings for the *Child*.

Features	*Child*	*Parent*
Create Child Account		x
Approve App Downloads		x
Set Screen Time Limits		x
Manage Google Activity Controls	Limited	x
Enable SafeSearch		x
Monitor Location		x
Access to Google Services	x	x
Modify Personal Info	Limited	x
Manage App Permissions	Limited	x
Control YouTube Settings	Limited	x
Adjust Google Ads Settings	Limited	x
Use Google Assistant	x	x
Access Communication Tools	x	x

name, password, or email can only be done by the parent. (3) *Manage app permissions:* modifying permissions may be restricted, or it requires parental approval. (4) *Control YouTube settings:* children may be able to use YouTube or YouTube Kids within parameters set by the parents. (5) *Adjust Google Ads settings:* children may be able to toggle some settings of the ads they see, but comprehensive ad settings are often controlled by the parent.

4 Study II: Qualitative Study

To study users' motivations toward using collaborative family apps and their perceptions of privacy on the apps, we conducted a follow-up qualitative study. In this phase, we captured users' insights into what motivates them to use collaborative family apps, their perceptions of privacy when using the app and their different virtual roles, and, finally, whether family apps impact their family relations in any way.

We selected Apple's Family Sharing as a running case study because Apple's Family Sharing is exclusive to Apple devices and is not accessible on Android, setting it apart from other apps. We wanted to explore families' experiences using a collaborative app that specifies a shared ecosystem. Additionally, research that focuses on Apple's devices is significantly underexplored, making this study an important contribution to understandings of its distinct capabilities and user experiences. Moreover, as we explored in Study I, other collaborative family apps share similar core features.

4.1 Recruitment and Screening

We conducted a screening survey on the User Interviews platform [55], which enabled us to reach diverse demographics. The platform allowed recruitment from a variety of countries, specifically the United States, the United Kingdom, South Africa, Canada, Germany, France, and Australia. We chose to retain all eligible participants from these countries—rather than limit our study to one country—in order to capture a broader range of parental experiences with Apple Family Sharing. This approach enhanced the diversity and applicability of our findings within the geographical constraints imposed by the platform (see also Section 6.5 for a discussion of this limitation). A total of 35 parents responded to the screening survey. Of these, 20 participants (57%) were selected to take part in the study, as this number was sufficient to reach data saturation, that is, where no new themes or insights were emerging. Participants were eligible if they were available, used Apple's Family Sharing, completed all questions in the screening survey, and had children. The survey included questions about their use of family apps, the devices connected to these apps, and their family structure (e.g., number of family members and their roles). Demographic information such as gender, marital status, living situation, education level, number of children, and household income was automatically provided by the platform through participant profiles.

4.2 Ethical Considerations

Our academic institution concluded that prior ethics approval was not required, as no personally identifiable information or similarly protected identifiable data was collected from the participants and the study did not directly involve minors. We followed the guidelines of our institution and the best practices of conducting ethical research in Computer Science [33]. All participants were provided information sheets describing the details about the data collection and storage practices. We encouraged participants to contact us for any questions before and after the interview sessions if they had any concerns related to the privacy of their data or other matters.

A potential ethical consideration in this study is that parents may have shared information about their children during interviews that the children themselves might not have consented to disclose. The nature of household technologies and parenting often led to discussions that included children's behaviors and preferences surrounding privacy. To mitigate this concern, we did not collect identifiable information about children. We focused on parents' reflections on technology use within the family context.

4.3 Participants

Participants were aged between 32 and 57 years old (mean = 42.6, SD = 7.2) from the United States of America (80%), United Kingdom (15%), and Germany (5%); 65% were women, and 35% were men. While 80% of the parents were married or in a civil union, 15% were either divorced or separated, and 5% had never married. Furthermore, 70% of parents lived with their husband or wife, 15% lived with a significant other, and 10% lived alone. All of the parents had children: the majority of the parents (45%) had an adolescent child, and 40% had a school-aged child; more details can be found in Table 4 (for detailed tables, see Appendix 8.3).

All parents had used Apple's Family Sharing App for at least 9 months, and they used at least two features of the app. Moreover, 85% used other family apps (e.g., 25% used Family 360, 25% used Google Family Link, 20% used Microsoft Family Safety, and 15% used Qustudio). Most of the parents (70%) connected Apple's Family Sharing app to at least 3 devices with at least 3–4 members using the app. Most parents (95%) shared one or more devices with family members; more details can be found in Table 5. The family app features' details and compatibility platforms can be found in Appendix 8.4.

4.4 Interview Sessions

We conducted semi-structured interviews remotely from April–May in 2022. The interview sessions were 45–50 minutes long on average. Parents were compensated through the User Interviews platform with gift cards worth 30 USD after completing the interview sessions. Interviews were audio-recorded and transcribed by a third-party company. The interviews were then proofread for syntax issues.

4.5 Qualitative Data Analysis

The semi-structured interviews covered the following topics: (1) household arrangements, (2) using collaborative family apps, (3) perception of privacy on the app, (4) understanding of functionalities on the app (e.g., creating accounts, sharing information, devices connected to the app), (5) privacy configurations of features on the app, (6) and impacts on family relations due to using family apps. Several topics were aimed at indirect data collection, such as questions about children's privacy expectations, device usage, and reactions to features like Screen Time and Ask to Buy. These questions sought to capture parental interpretations of their child's experiences, rather than direct input from the children themselves.

The complete interview guide is presented in Appendix 8.2 and a summary of central topics in Table 6.

The interface changes between 2022 and 2024 do not impact the findings of our interview study, as participants were not asked specifically about the app's interface. Instead, the focus was on their overall experience with the app and how it affected their lives and relationships. Additionally, the core functionalities of the app have remained consistent year to year, ensuring that any design updates do not alter the key insights drawn from the participants' experiences.

To analyze the semi-structured interviews, we adopted a hybrid approach [28, 61]. We used ATLAS.ti [17], qualitative data analysis

Table 4: Participant Characteristics: Age, Gender, Occupation and Members Using the App. The age categories are as follow: *Infant* (<1 year), *Toddler* (1–3 years), *Preschooler* (4–5 years), *School-aged* (6–12 years), *Adolescent* (13–17 years), and *Adult* (18+ years). The number of children is denoted in between parentheses (e.g., (1) Adolescent).

#	Age	Gender	Occupation	Members Using the App
P01	40	Man	Data Analytics Analyst	Mother, Father, (2) School-aged, Grandmother, Grandfather
P02	39	Woman	Manager/Assistant Manager	Mother, (3) Unknown ages*
P03	37	Man	Business Analyst	Mother, Father, (1) Preschooler
P04	45	Man	Machine Maintenance Mechanic	Mother, Father, (1) Adolescent; (1) Adult
P05	50	Woman	Office Manager	Mother, Father, (1) Adolescent, (1) Adult
P06	38	Woman	Personal Care Worker	Mother, Father, (4) Adolescent, (1) Toddler
P07	36	Woman	Registered Nurse	Mother, (1) School aged
P08	49	Woman	Consultant	Mother, (2) School-aged
P09	45	Woman	Teacher/Teacher Trainer	Mother, Father, (1) School-aged; (2) Adult
P10	35	Woman	Certified Personal Trainer	Mother, (1) School-aged, (1) Adolescent
P11	35	Woman	Speech Language Pathologist	Mother, Father, (2) Toddler
P12	37	Woman	Manager	Mother, Father, (1) Preschooler
P13	55	Man	Chief Operating Officer	Mother, Father, (1) Adolescent
P14	44	Man	Digital Director	Mother, Grandmother, (2) School-aged
P15	46	Man	Supervisor	Father, (2) Adolescent
P16	57	Woman	Home maker	Mother, Father, (1) Adolescent
P17	52	Woman	Engineering Program Manager	Mother, (1) Adolescent, (1) Adult
P18	44	Woman	Teacher	Mother, Father, (1) Preschooler, (1) School-aged, (1) Adolescent
P19	32	Woman	Office Personnel	Mother, Father, Grandmother, (1) Preschooler
P20	36	Man	Critical Care Registered Nurse	Father, (1) Preschooler, (1) School-aged, (1) Adolescent

Table 5: Participant device and app use based on screening survey responses:

Device(s) and app use	N = 20	%	Device(s) and app use	N = 20	%
Apps Used (Other Family Apps)			*Features from other apps*		
Google Family Link	5	25%	Location Tracking	14	70%
Family 360	5	25%	Screen Time	11	55%
Microsoft Family Safety	5	25%	Content Filters	8	40%
Qustudio	3	15%	Media	6	30%
iSharing	4	20%	Cloud Space	7	35%
Norton Family Parental Control	4	20%	Apps and Subscriptions	8	40%
Others	7	35%	*Features Used (Apple's Family Sharing)*		
Do not use other apps	2	10%	Apple Music	14	70%
Family members using Family Sharing			iTunes and App Store Purchases	16	80%
1 - 4 members	15	75%	iCloud Storage	16	80%
More than 5 members	25	5%	Location Sharing	17	85%
Number of Devices Connected			Screen Time	12	60%
iPhone	20	100%	Others	2	10%
iPad	16	80%	*Role on (Apple's Family Sharing)*		
MacBook (Air, Pro)	13	65%	Organizer	8	40%
Apple Watch	6	30%	Parent/Guardian	12	60%
iMac	4	5%	*Duration to use Apple's Family Sharing (years)*		
Role in Family			Less than 1 year	3	15%
Parents	18	90%	1 - 2 years	8	40%
Older Sibling, Uncle/Aunt	1	5%	3–4 years	3	15%
Other	1	5%	more than 5 years	4	20%

Table 6: Summary of central interview topics, research intentions, and sample questions from interview script.

Topic(s)	Research Intention	Sample questions
Households, Permissions, Individual Privacy	To understand how individual privacy is defined vs. collective use of the app as a family	*Do you have any concerns about your own privacy being affected by Family Sharing?*
App Function, Connected Devices, Features	To understand how users use the app to translate their needs	*Have you set some information to be hidden from other family members?*
Configurations, Disabling, Enabling Sharing	Participants' thoughts on controlling privacy configurations on the app	*What happens when you stop sharing on Family Sharing?*
Impacts, Effects, Family relations	Participants' perception of how the app may impact their family relationships	*Do you think using Family Sharing can affect your relationship with your child?*

software, to support the systematic organization, coding, and retrieval of data. This tool was selected for its ability to manage large volumes of qualitative data efficiently and to facilitate collaborative coding through structured codebooks and memoing features. Prior to coding the interviews, the two authors agreed on higher-level categories for the code book. The higher-level categories corresponded to the main topics of the interview guide: motivations to use family apps, sharing content with family members, features and functionalities of the app, privacy configurations, setup, and effects of using family apps. The first author proceeded to code two interviews with higher-level codes and noted inductive codes that emerged. The first and second authors discussed the codebook and generated a new codebook that was used to code two more different interviews. The two authors discussed the codebook again, and since no more codes were introduced, the first author completed the coding of the remaining interviews using the finalized codebook. The final codebook can be found in Appendix 8.5.

5 Study II: Results

The themes identified in this study are in the context of Apple's Family Sharing: *Facilitating Family Connection and Content Sharing*, *Navigating and Interpreting Privacy Settings*, and *Influence of Collaborative Family Apps on Families*. However, these themes transcend the boundaries of a single platform. The themes illuminate broader patterns of family interactions, privacy management, and the potential impacts of the usage of collaborative family apps on families.

5.1 Facilitating Family Connection and Content Sharing

Collaborative family apps like Apple's Family Sharing have been integrated into families' routines. Collaborative family apps have been shown to facilitate communication, such as calendars and events and sharing of content, including pictures and videos. Participants discussed how they shifted from traditional parental control apps to collaborative family apps, using screen management tools for parenting, and location-sharing features for additional reassurance about their children's whereabouts.

5.1.1 Shifting from Parental Control Apps to Collaborative Family Apps. Nearly half of the participants (13/20) reported transitioning from traditional parental control apps to collaborative family apps, such as Apple's Family Sharing. Parents cited the following motivations for this shift: location sharing, budgeting, app purchases, screen time management, and ease of use of the app. The primary motivation for this shift, however, was the shared ecosystem in the household, where all the family members used Apple devices.

One parent described how device compatibility in the household shaped their experience: "*I used Google [referring to Google's Family Link app] for a while but Apple is just more convenient because I have the iPad and then a MacBook and an iPhone so everything kinda just syncs, so I pretty much use Apple now ... I'm a mom of three so easy is [laughing] what I look for*" (P07).

We also observed that when one parent used a different device model, such as an Android phone, the parent with the Apple device took on the role of the primary parent on the app.

5.1.2 Screen Time Management as a Parenting Tool. Almost half of the parents (15/20) used the collaborative app's screen time management feature as a rewarding system or discipline tool for children. During the COVID-19 pandemic, this feature became critical for managing routines: "*Lately what has happened with COVID, the first year and a half kids were being schooled from home, and so that's almost messed up everybody's sleep time. I make my husband do it [set screen time restrictions] because I'm always a bad person otherwise*" (P14). Screen time management is not a particularly new feature in family digital apps; it has been one of the staple features of parental control apps. However, in the context of collaborative family apps like Apple's Family Sharing, our findings revealed a desire for more granular controls. This includes features like per-app time restriction and the ability to customize limits based on specific app categories, such as social media apps.

5.1.3 Location Sharing as a Safety Assurance. The majority of parents (14/20) emphasized the importance of location sharing; this was driven by safety concerns. These concerns ranged from wanting to stay informed about their children's whereabouts to more extreme fears, such as human trafficking. "*Spooky scary things that you hear on the news. I'm a high school teacher, so students go missing, and I'm concerned because I know all teenagers basically have a cell phone and I don't know why they can't find them. We've got sex trafficking everywhere. So that raises an alarm for me*" (P18).

5.1.4 Sharing A Virtual Space. Several participants described the convenience of shared photo albums or cloud space, but with hesitation about losing control over what gets seen. *"I would share to the shared album because, you know, it makes it easier… but I also don't want everyone to see everything"* (P09). And *"Your personal files are private until you share them, and then the app doesn't always tell you who exactly can see them"* (P13).

The embedded nature of Family Sharing in the Apple ecosystem further influenced these decisions. Participants described switching to it from other apps due to device compatibility, with privacy decisions influenced more by infrastructure than intent. *"I do just* *because, but I kind of cast [privacy concerns] away because it's convenient"* (P06).

5.1.5 Selective Sharing and Workarounds. Several participants described creating personal workarounds to avoid oversharing. This included manually excluding sensitive photos from shared albums, avoiding family cloud storage, or using external tools for private communication. *"I avoid putting things in shared albums if they're personal, I just send them directly"* (P08). And *"I like that you can pick what to share... but I'm never really sure if it worked"* (P14).

5.2 Navigating and Interpreting Privacy Settings

The use of collaborative family apps, such as Apple's Family Sharing, revealed confusion and concern about the app's privacy controls, including role-based access, data visibility, and shared information boundaries.

5.2.1 Role Hierarchies and Misunderstandings. While many parents understood the basic difference between *Child* and *Adult* roles, few were confident about what each role could access or control. Most parents (11/20) understood the differences between the *Parent/Guardian* role and the *Child* role, roles such as *Organizer*, *Parent/Guardian*, and *Adult* caused confusion, such as the assumption that there is no difference between the latter two roles, and how much control these roles have over users' privacy on the app. This confusion led to unintentional disclosure and control mismatches. *"My husband is listed as an adult but not a parent or organizer, and I had no idea that meant he couldn't approve anything for the kids"* (P06). And *"There are too many layers. I wish it just said what each person could do"*(P11).

5.2.2 Perceived Data Retention and Transparency. Participants expressed uncertainty about what happens to data once sharing settings are changed. Many were unsure whether previously shared data remained accessible. Parents speculated about how the collaborative family apps handle data when features such as iCloud and Location Sharing are disabled (for example, wondering if after disabling iCloud, personal data might still be stored somewhere but cannot be accessed). Others suspected that personal data can be retained by the app, despite this feature being turned off. A few other parents also believed that family members can still access older locations, or that other family members can see each others' locations despite it being disabled in the app. *"Even if I turn off iCloud, does that mean the other person can't still see what was already there? I don't know and it's not clear"* (P17). And *"It doesn't tell you what will happen after. And if it's saying it in the fine print, who reads those? We just click agree"* (P06).

5.2.3 Accidental and Interdependent Sharing. Participants reported that data sometimes became visible to others unintentionally. Examples included shared calendars, synced photos, and app activity being accessible across accounts. *"My partner got mad because something showed up on our shared calendar that I didn't mean to share"* (P19). And *"Probably if a man or a woman forgot that they were sharing their location, that would be a privacy issue"* (P11).

Some parents (9/20) described that they did not know how to restrict information-sharing effectively.

5.2.4 Financial Data and Trust. Several participants expressed concern about shared financial data, such as credit card information being visible to others in the family group. *"Why can only one person use a card? It makes no sense. We argued about whose card to use"* (P12). And *"I trust Apple more than I trust my kid with my card, but I do wonder if the data sticks around after I remove it"* (P10).

5.2.5 Temporal Dimensions of Privacy. Participants questioned the longevity of shared information after removing a family member or disabling sharing features.*"When you remove someone from Family Sharing, can they still see your location?"* (P09). And *"I worry about how long the app remembers things we shared before"* (P13).

5.3 Influence of Collaborative Family Apps on Families

Collaborative family apps like Apple's Family Sharing impacted family dynamics by influencing how boundaries and relationships are negotiated. These apps can influence trust, autonomy, and control within households. While these apps enhance transparency and improve communication, they can also introduce sources of tension related to privacy and financial conflicts.

5.3.1 Effects on Parent-Child vs. Parent-Other Parent/Partner. Family Sharing mediated two distinct types of interpersonal relationships in the home: those between parents and children, and those between parents or adult partners. Participants described unique privacy tensions and expectations within each relationship type. These tensions were shaped by role assumptions, monitoring expectations, and degrees of digital literacy.

In parent-child dynamics, parents exercised a high degree of control and oversight, often justifying this based on the child's age or perceived lack of judgment. Children were expected to adapt to configurations set by adults, sometimes without full awareness of what was being shared or visible. "*I can see my two daughters' locations and then all their devices, so even their AirPods, their iPads, their iPhones. She [one of his daughters] got her first boyfriend a couple months ago, I could see she was visiting his house so I drove by his house and they didn't know. [When asked if the daughters voluntarily share their location, the participant replied:] I pay their bill*" (P15).

In contrast, relationships between co-parents or adult partners introduced more complex negotiations around control, autonomy, and privacy boundaries. These dynamics were more reciprocal and often revealed tensions or suspicions when visibility or control settings were misaligned or unclear. *"Yeah because if they're going through pictures and you know that they're gonna find stuff they don't want to see"* (P11).

5.3.2 Cultural and Gendered Variations in Privacy Expectations. Privacy norms varied across different cultural backgrounds. As an example, P20, an African-born parent, contrasted her upbringing with European norms, reflecting on the use of the app. "*I think European culture is different from where I'm coming from, so I'm an African, you know. I was born in Africa although I was raised in Europe. I always tell my kids, for example, I was born in Africa, you were born in Europe, doesn't mean that you can misbehave or do whatever you like. Yeah, privacy is paramount; however, their safety* *for me supersedes that. It's irrespective of how they feel as invasion of privacy*" (P20).

Several parents (6/20) changed their parenting strategies on the app based on their children's age and gender, impacting the level of privacy they allowed the child on the app. Participants thought that younger children required more strict rules because of their age and lack of awareness of digital risks. Parents expressed greater concerns for daughters compared to sons. *"She's a girl, so I'm more cautious. I check her location more. With my son, I'm not that worried"*(P17).

5.3.3 Relationship Tensions and Privacy Boundaries. Participants recounted relationship strain due to mismatched assumptions about what was visible to whom, or when a change in settings triggered suspicion or conflict. These situations often revealed underlying privacy expectations that were not aligned. "*My husband didn't know I turned off iCloud syncing. He got suspicious and asked what I was hiding*" (P06).

5.3.4 Digital Consent and Unawareness. Participants expressed concern that other family members, particularly children or older adults, were unaware of the extent of data being shared or monitored. This lack of awareness undermined the possibility of informed consent within the family network. *"My daughter didn't even know I could see her app activity" (P11).*

5.3.5 Device Sharing and Cross-Account Visibility. Participants described how shared devices, such as iPads or computers, created unexpected visibility into private content like calendars, messages, or photos. This overlap between accounts and devices created accidental exposure. *"I didn't know my calendar was syncing to his device too" (P08).* Parents also maintained the passwords of their children's account even if they were part of the app: "*I know their passwords to their phones, so I have to be able to watch them and Find My iPhone*" (P16).

6 Discussion

This study explored the use of collaborative family apps to navigate family dynamics and privacy needs. The study answers the following research questions: (RQ1) *How do families translate their needs through collaborative family apps*? (RQ2) *How do family members understand the privacy settings of collaborative family apps?* and (RQ3) *What are the impacts that collaborative family apps have on family relationships*? We examined these research questions by conducting a comparative analysis of collaborative family apps and parental control apps, with a focus on Apple's Family Sharing and Google's Family Link. We then identified through our qualitative study why families shift to collaborative family apps, and how they manage their privacy expectations and boundaries on the app. Our findings reveal usability issues with these apps, which impact families in different ways.

6.1 Why Collaborative Family Apps (RQ1)

Sociological research has extensively examined the changing dynamics in modern families and the privacy of digital spaces [51, 93]. Technologies have also led to new forms of communication [36]. In collaborative family apps, we observe that this shift impacts how parents translate their needs on the apps, and how they negotiate privacy with children. There is a shift from using the app individually to engaging with it as a collaborative tool. This transition appears to be driven by the functionalities participants found useful—such as shared purchases and managing a common vendor—as well as the overall ease of use enabled by Apple's mature ecosystem. While these align with factors often associated with technology adoption [31], participants emphasized practical convenience and social coordination over abstract models. However, collaborative apps also bring a range of privacy risks that distinguish them from other contexts. Parents voiced concerns about unintended visibility into each other's purchases, the inability to fully control what family members can access or view, and the potential for overstepping boundaries and the impact the app may have on family relations by creating tensions driven by the use of the app.

The study also explored two very popular collaborative apps: Apple's Family Sharing and Google's Family Link. Collaborative Family apps play a significant role in defining family roles, both in real life and in the virtual space. For example, Apple's Family Sharing offers four distinct roles, while Google's Family Link provides two. Our data revealed that participants often found the various roles on Family Sharing confusing. This highlights the importance of designing digital roles that are intuitive and align with how families understand and navigate their responsibilities. When users clearly understand the scope and control associated with each role, it can significantly influence the privacy settings they choose for themselves and others, ultimately shaping how families manage their shared digital spaces.

Both Apple's Family Sharing and Google's Family Link include parental control features, such as app purchase approvals for children and screen time management. However, the apps differ in areas like ecosystem compatibility. Our interviews revealed that parents who did not share the same digital ecosystem as their family members were often excluded from the parenting process on the app (e.g., if all the family members are using Apple devices and one parent is using an Android device). This creates a significant barrier to using these tools, as non-ecosystem parents are unable to participate fully. A potential solution could be to design cross-platform compatibility, enabling parents using different ecosystems to engage equally in managing family settings and controls.

6.2 Managing and Negotiating Privacy Boundaries (RQ2)

Families' privacy expectations were fluid and contextually dependent. Participants often had implicit norms about what should or should not be visible, but the app's defaults did not always match those norms. For instance, shared photo albums, calendar entries, and financial data sometimes led to accidental exposure, especially when users misunderstood role-based permissions.

This mismatch between users' privacy expectations and actual configurations suggests that privacy boundaries are fuzzy and relational [83, p.337], rather than fixed. Role misunderstandings (e.g., thinking that *Adult* and *Organizer* had equivalent powers) contributed to unexpected visibility, and participants lacked clarity about what data persisted after settings were changed or members were removed. Such uncertainty challenged the legibility and predictability required by Contextual Integrity [75, 76].

Participants' decisions reflected a Privacy Calculus [60], in which users weighed the potential privacy risks—such as visibility into purchases or location—against perceived benefits like convenience, parental reassurance, and smoother family coordination. As one participant summarized, "*I cast privacy concerns aside because it's convenient.*" However, in the context of Family Sharing, this calculus is shaped by two interrelated dimensions. First, the app context introduces specific tradeoffs: participants sought conveniences like centralized purchases or parental control, but faced costs such as a lack of granular control and unintended exposure of personal content. Second, the interpersonal dynamics of family life added complexity to privacy decision-making. Participants were not only evaluating risks for themselves but also for (and from) other family members—introducing a layer of *collective* interpersonal privacy.

These complexities surfaced in selective sharing behaviors and workarounds that participants opted for to avoid *oversharing*, (e.g., excluding sensitive photos from shared albums). These workarounds were often ad hoc, reflecting uncertainty about the app's default settings and limited visibility into who could access what information. These practices suggest a nuanced negotiation of privacy within the collaborative environment, where users selectively engage with features based on their trust in the system and their confidence in understanding its boundaries.

The *Organizer* is the virtual head of the household, or the admin, who can control the app usage of other members. We explored participants' level of understanding what each role can do, including the role of the *Organizer.* Our findings revealed misunderstandings around the privacy controls of different roles on the app, such as *Parent/Organizer* vs. *Adult.* As covered in the first study, we observed that different roles in the app have different levels of power to control the usage and data sharing of different features of other family members' devices. Misunderstanding what each role can do can potentially risk establishing clear boundaries around shared information. Further research is needed to better understand how these virtual boundaries are negotiated with changing contexts and how these can affect family dynamics.

As seen from the data, location sharing not only fosters a sense of security but also reflects societal narratives of fear and risk that parents have, which are essential for children's safety. However, these tools also introduce potential tensions around trust and autonomy within families. Our findings about the negative impacts of monitoring are aligned with a prior line of research that examined parents monitoring children's device use. Studies suggest that children often express resentment [46, 47] and develop a need to maintain their privacy in relation to their parents [30, 59].

6.3 Collaborative Family Apps and Family Dynamics (RQ3)

Collaborative parental apps mediated two distinct relational dynamics: parent-child and co-parenting (or parent–other adult) relationships. These relationships were impacted differently:

Monitoring tools like location sharing or screen time controls often amplified power asymmetries in parent-child relations. Children adapt to adult configurations ("Ask to Buy" and screen time restrictions) and parental justifications ("*I pay the bill*"). Differential treatment based on age and gender also emerged, with daughters being more closely monitored than sons, shaped by both safety concerns and cultural norms. Parents justified monitoring as a privilege tied to financial responsibility. Yet, the monitoring aspect was often perceived by children and teens as distrustful. This perception aligns with existing literature on digital surveillance in families, which has shown that monitoring can strain parent–child relationships and provoke resistance, negotiation, or disengagement from technology use altogether (e.g., [26, 44, 84, 101, 106]).

These dynamics reflect a form of Interdependent Privacy (IDP) [21], where one individual's decisions (e.g., a parent's configurations) shape another's privacy experience. Prior work on IDP often focuses on sharing others' data—such as in smart homes, social media, or genomics—but this study reveals an underexplored angle: the restriction of one's own ability to share personal data. For example, a child may be unable to access or post to social platforms or use location-based features, not by choice but due to parental control settings. This reversal of typical IDP framing—where the constraint lies not in data disclosure but in the denial of autonomy to disclose—highlights how collaborative family apps may mediate privacy for others beyond one's own privacy.

Participants reported tensions stemming from unclear boundaries and accidental disclosures between parent-other parent/partner relationship dynamics (e.g., financial info or synced calendars). These incidents suggest that even among adults, trust and control are negotiated, not given—reinforcing that collaborative apps are not neutral tools but active agents in relational power dynamics.

6.4 Recommendations and Design Implications for Collaborative Family Apps

Based on the study findings, we provide actionable design recommendations to guide the development of collaborative family apps:

6.4.1 Navigating autonomy and supervision in digital parenting. Collaborative family apps should offer more granular controls. Participants shared that they wanted per-app screen time limits and customizable monitoring that can be adjusted with the child's age [54] or good behavior [102]. Although collaborative family apps offer monitoring features, some parents still felt compelled to manually check their child's device—often by knowing the child's password—as a way to ensure safety and oversight. Rather than relying solely on technical control, families could benefit from co-creating rules and fostering open communication about why certain boundaries [54, 78], such as password sharing, may be necessary in specific situations (e.g., a parent describing finding inappropriate websites on their child's device). These methods could foster more trust and open communication in households.

6.4.2 Misunderstanding of hierarchies and data practices. To minimize unintentional conflicts, accidental sharing, or unclear role distinctions (what each role can access or control), collaborative family apps could offer personalized nudges [92], short and clear descriptions, or a simplified taxonomy [38] to each user on the different roles and how the other roles impact the individual's device. This might include, for example, narratives and story telling [105], such as incorporating real-life scenarios of what different access and controls roles have (e.g., *Organizers* can can assign a role to others, while *Adults* cannot do that, while both of these roles can approve the purchases of someone with a *Child* role).

The app can provide information to users when a privacy configuration is changed, in order to let them know what has happened with to their data. For example, if a parent chooses to disable purchase sharing, the app should notify the family member about what happens to their personal information, such as credit card data.

Additionally, collaborative family apps can provide educational content on apps that is specific to different areas and topics, like online safety, culturally sensitive materials for privacy and other relevant topics for parents.

6.4.3 Diverse family structures and cultural norms. Collaborative family apps could introduce customization to payment settings to accommodate various family needs, such as: (1) allowing more members on the app to add their payment information to manage purchases on the app, to ease the burden of the purchases on a single user, and (2) providing an option for older children to also contribute to app purchases, to further support children's autonomy. Prior research has discussed the communication gap between parents and children due to variations in technology perspectives; while children are more familiar with technologies, they are less responsible [30]. Teens are more likely to check their own app safety than listen to their parents [3]. Therefore, children and teens that interact more actively within the app may also be rewarded with more privileges or privacy features there.

Collaborative family apps should also acknowledge variations in privacy norms between cultures (e.g., African vs. European culture). For example, while some cultures may value shared access over individual privacy, other cultures may emphasize personal boundaries more. This could potentially mean including more controls to determine which data is shared with whom on the app (e.g., sharing location during certain times when it is more risky, such as nighttime).

6.5 Limitations

This work reports on children's experiences through their guardians, rather than directly from the children. These interpretations may not always accurately reflect the children's perspectives. Obtaining informed consent from minors can be challenging, as researchers have questioned whether consent is genuinely informed when it is provided on behalf of children by their parents [34, 72]. Additionally, the interview questions in this study were designed to capture nuanced aspects of family dynamics and app privacy. Simplifying these questions for use with minors could have risked misinterpretation of the complex privacy scenarios we aimed to explore. We acknowledge this as a limitation and recognize the importance of developing age-appropriate methods to directly engage children in future research.

We also recruited families who used Apple's Family Sharing feature, which is exclusively available on Apple devices, and this was further constrained by the recruitment platform we used. Our participant pool aligns with the higher household income typically observed among U.S. iPhone users, whose median household income is approximately $85,000 annually [29]. While these constraints were necessary due to both the technical requirements and the recruitment platform, it is important to recognize that this may limit the generalizability of our findings to broader populations, including those with lower incomes or users of other collaborative family apps on different device ecosystems.

Our study included 20 participants from the U.S., U.K., and Germany, which allowed us to examine a range of perspectives on privacy and usability in Apple's Family Sharing. While Apple's Family Sharing app operates as a standardized system globally, cultural differences in family communication, privacy norms, and parental monitoring practices may shape how users interact with the platform. For example, our findings highlighted variations in privacy expectations and parental control attitudes based on cultural background, such as stricter monitoring of daughters versus sons or differing views on children's autonomy (see, e.g., P20's reflection on African versus European norms). While these insights provide valuable initial observations, a larger cross-cultural study would be necessary to systematically analyze the significance of cultural differences in Collaborative Family Sharing apps usage.

7 Conclusions

This work explores how families use collaborative family apps, in particular Apple's Family Sharing and Google's Family Link, to navigate their communication and privacy dynamics. By addressing how families reflect on their needs, understand privacy settings, and experience the impacts of these apps, this work sheds light on the evolving role of technology in families' lives.

The findings revealed that critical parenting tools like location sharing and screen time management were useful, yet led to some mishaps between family members. Families expressed misunderstandings around the privacy settings and the role hierarchies of the app, leading to accidental sharing and mistrust. Furthermore, collaborative family apps mediate family communication and dynamics, but they can also create disagreements around monitoring, financial matters, and privacy expectations. Cultural and gendered variations shaped the usage of the app, with stricter controls for younger children and daughters.

This work contributes to the body of technology-mediated family interactions by: (1) an in-depth comparison of popular collaborative family apps and an examination of their functionalities, (2) exploring why families use collaborative family apps and how they translate their needs on the apps, (3) highlighting privacy and usability challenges with these apps, which could strain family relationships, (4) providing insights into different cultural and gender-based challenges that shape family uses of the app, and (5) providing recommendations and design implications for app developers and researchers that reflect family needs through collaborative family apps.

Acknowledgments

This work was funded by the Research Council of Finland via grant numbers 345991 and 345992. We are grateful to all study participants for their time, experiences and insights. We note that *My Data or Our Data? A Comparative Study of Collaborative Family Apps and Parents' Experiences with Apple's Family Sharing* is an independent publication and has not been authorized, sponsored, or otherwise approved by Apple Inc. or Google LLC.

References

[1] Noura Abdi, Xiao Zhan, Kopo M Ramokapane, and Jose Such. 2021. Privacy norms for smart home personal assistants. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. ACM, Association for Computing Machinery, Virtual Event, 1–14.

[2] Kaitlin Ahern. 2023. How Much Screen Time Is Too Much For Kids? *Forbes*. https://www.forbes.com/health/family/how-much-screen-time-kids/ Accessed: 2023-08-22.

[3] Mamtaj Akter, Amy J Godfrey, Jess Kropczynski, Heather R Lipford, and Pamela J Wisniewski. 2022. From Parental Control to Joint Family Oversight: Can Parents and Teens Manage Mobile Online Safety and Privacy as Equals? *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW1 (2022), 1–28.

[4] Mahdi Nasrullah Al-Ameen, Huzeyfe Kocabas, Swapnil Nandy, and Tanjina Tamanna. 2021. "We, three brothers have always known everything of each other": A Cross-cultural Study of Sharing Digital Devices and Online Accounts. *Proceedings on Privacy Enhancing Technologies* 2021, 4 (2021), 203–224. https://doi.org/10.2478/popets-2021-0067

[5] Turki Alelyani, Arup Kumar Ghosh, Larry Moralez, Shion Guha, and Pamela Wisniewski. 2019. *Examining parent versus child reviews of parental control apps on google play*. Vol. 11579 LNCS. Springer International Publishing, Cham, Switzerland. 3–21 pages. https://doi.org/10.1007/978-3-030-21905-5_1

[6] David E Alexander. 2014. Social media in disaster risk reduction and crisis management. *Science and engineering ethics* 20 (2014), 717–733.

[7] Ahmed Alshehri, Eugin Pahk, Joseph Spielman, Jacob T Parker, Benjamin Gilbert, and Chuan Yue. 2023. Exploring the Negotiation Behaviors of Owners and Bystanders over Data Practices of Smart Home Devices. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (Hamburg, Germany) *(CHI '23)*. Association for Computing Machinery, New York, NY, USA, Article 67, 27 pages. https://doi.org/10.1145/3544548.3581360

[8] Anonymous. 2025. Supplementary Materials for "My Data or Our Data? A Comparative Study of Collaborative Family Apps and Parents' Experiences with Apple's Family Sharing". https://osf.io/fc58q/?view_only=2cb9d3beadf6495fab05089a0bbb462f Open Science Framework, view-only link.

[9] Jamal Abdul Nasir Ansari and Nawab Ali Khan. 2020. Exploring the Role of Social Media in Collaborative Learning: The New Domain of Learning. *Smart Learning Environments* 7 (2020), 9. https://doi.org/10.1186/s40561-020-00118-7

[10] Apple. 2020. *Share your location with your family*. Apple Inc. Retrieved April 8, 2022 from https://support.apple.com/en-gb/HT201087 Web link.

[11] Apple. 2021. *Create an Apple ID for your child*. Apple Inc. Retrieved April 8, 2022 from https://support.apple.com/en-us/HT201084 Web link.

[12] Apple. 2021. *What is Family Sharing?* Apple Inc. Retrieved April 8, 2022 from https://support.apple.com/en-us/HT201060 Web link.

[13] Apple. 2021. *What types of content can I share with my family?* Apple Inc. Retrieved April 8, 2022 from https://support.apple.com/en-gb/HT203046 Web link.

[14] Apple. 2022. *Family Sharing Official*. Apple Inc. Retrieved January 31, 2022 from https://www.apple.com/family-sharing/ Web link.

[15] Apple Inc. 2025. Search on the App Store. https://developer.apple.com/app-store/search/. Accessed: 2025-03-23.

[16] AppleInsider. 2024. Apple's Active Devices. https://www.appleinsider.com. Accessed: 2024-08-26.

[17] ATLAS.ti Scientific Software Development GmbH. 2023. *ATLAS.ti Cloud: The Web-Based Qualitative Data Analysis Software*. ATLAS.ti Scientific Software Development GmbH. https://cloud.atlasti.com Cloud version.

[18] Aura. 2025. Aura Parental Control. https://www.aura.com/parental-controls. Accessed: 2025-03-26.

[19] Bark. 2022. *Bark*. Bark Technologies, Inc. Retrieved January 31, 2022 from https://www.bark.us Web link.

[20] Mikael Beyene, Philipp A Toussaint, Scott Thiebes, Matthias Schlesner, Benedikt Brors, and Ali Sunyaev. 2022. A scoping review of distributed ledger technology in genomics: thematic analysis and directions for future research. *Journal of the American Medical Informatics Association* 29, 8 (2022), 1433–1444.

[21] Gergely Biczók and Pern Hui Chia. 2013. Interdependent privacy: Let me share your data. In *Financial Cryptography and Data Security: 17th International Conference, FC 2013, Okinawa, Japan, April 1-5, 2013, Revised Selected Papers (Lecture Notes in Computer Science, Vol. 7859)*. Springer, Okinawa, Japan, 338–353.

[22] Michele C. Black, Kathleen C. Basile, Matthew J. Breiding, Sharon G. Smith, Mikel L. Walters, Melissa T. Merrick, Jieru Chen, and Mark R. Stevens. 2010. National Intimate Partner and Sexual Violence Survey.

[23] Amel Bourdoucen and Janne Lindqvist. 2024. Privacy of Default Apps in Apple's Mobile Ecosystem. In *Proceedings of the CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '24)*. Association for Computing Machinery, New York, NY, USA, Article 786, 32 pages. https://doi.org/10.1145/3613904.3642831

[24] Shantel Gabrieal Buggs. 2022. 241Negotiating Intimacy via Dating Websites and Apps: Digital Media in Everyday Life. In *The Oxford Handbook of Digital Media Sociology*. Oxford University Press, Oxford, UK. https://doi.org/10.1093/oxfordhb/9780197510636.013.16 arXiv:https://academic.oup.com/book/0/chapter/337807202/chapter-ag-pdf/57122145/book_35410_section_337807202.ag.pdf

[25] Canopy USA, Inc. 2025. Canopy Parental Control App. https://canopy.us/. Accessed: 2025-03-26.

[26] Vicky Charisi, Nikoleta Yiannoutsou, Shuli Gilutz, Matthew Dennis, and Shyamli Suneesh. 2024. Designing for Children's Digital Well-being: An Agenda for Research, Policy and Practice. In *Proceedings of the 23rd Annual ACM Interaction Design and Children Conference* (Delft, Netherlands) *(IDC '24)*. Association for Computing Machinery, New York, NY, USA, 1026–1028. https://doi.org/10.1145/3628516.3661154

[27] Rahul Chatterjee, Periwinkle Doerfler, Hadas Orgad, Sam Havron, Jackeline Palmer, Diana Freed, Karen Levy, Nicola Dell, Damon McCoy, and Thomas Ristenpart. 2018. The spyware used in intimate partner violence. In *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, IEEE, San Francisco, CA, USA, 441–458.

[28] Victoria Clarke and Virginia Braun. 2013. *Successful Qualitative Research: A Practical Guide for Beginners*. SAGE Publications Ltd, London, UK.

[29] Inc. Comscore. 2024. iPhone Users Earn Higher Income, Engage More on Apps than Android Users. https://www.comscore.com/Insights/Infographics/iPhone-Users-Earn-Higher-Income-Engage-More-on-Apps-than-Android-Users. Accessed: 2024-09-12.

[30] Lorrie Faith Cranor, Adam L. Durity, Abigail Marsh, and Blase Ur. 2014. Parents' and Teens' Perspectives on Privacy in a Technology-Filled World. In *Proceedings of the Tenth USENIX Conference on Usable Privacy and Security* (Menlo Park, CA) *(SOUPS '14)*. USENIX Association, USA, 19–35.

[31] Fred D Davis, RP Bagozzi, and PR Warshaw. 1989. Technology acceptance model. *J Manag Sci* 35, 8 (1989), 982–1003.

[32] Katie Davis, Anja Dinhopl, and Alexis Hiniker. 2019. *"Everything's the Phone": Understanding the Phone's Supercharged Role in Parent-Teen Relationships*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3290605.3300457

[33] D Dittrich and E Kenneally. 2012. *The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research*. Technical Report. U.S. Department of Homeland Security. https://catalog.caida.org/paper/2012_menlo_report_actual_formatted

[34] Sue Dockett, Bob Perry, and Emma Kearney. 2013. Promoting children's informed assent in research participation. *International Journal of Qualitative Studies in Education* 26, 7 (2013), 802–828.

[35] Satu Elo and Helvi Kyngäs. 2008. The qualitative content analysis process. *Journal of Advanced Nursing* 62, 1 (2008), 107–115. https://doi.org/10.1111/j.1365-2648.2007.04569.x

[36] Ola Erstad, Kristinn Hegna, Sonia Livingstone, Oana Negru-Subtirica, and Mariya Stoilova. 2024. How digital technologies become embedded in family life across generations: scoping the agenda for researching 'platformised relationality'. *Families, Relationships and Societies* 13, 2 (2024), 164 – 180. https://doi.org/10.1332/20467435Y2024D000000023

[37] Álvaro Feal, Paolo Calciati, Narseo Vallina-Rodriguez, Carmela Troncoso, and Alessandra Gorla. 2020. Angel or Devil? A Privacy Study of Mobile Parental Control Apps. *Proceedings on Privacy Enhancing Technologies* 2020, 2 (2020), 314–335. https://doi.org/10.2478/popets-2020-0029

[38] Yuanyuan Feng, Yaxing Yao, and Norman Sadeh. 2021. A Design Space for Privacy Choices: Towards Meaningful Privacy Control in the Internet of Things. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. ACM, Association for Computing Machinery, Yokohama, Japan, 1–16.

[39] Mohamed Amine Ferrag, Leandros Maglaras, and Ahmed Ahmim. 2017. Privacy-preserving schemes for ad hoc social networks: A survey. *IEEE Communications Surveys & Tutorials* 19, 4 (2017), 3015–3045.

[40] World Economic Forum. 2023. *Risks to kids online are growing. Here's what we can do*. World Economic Forum. https://www.weforum.org/agenda/2023/08/risks-to-kids-online-are-growing/ Accessed: 2023-08-22.

[41] Diana Freed, Sam Havron, Emily Tseng, Andrea Gallardo, Rahul Chatterjee, Thomas Ristenpart, and Nicola Dell. 2019. "Is my phone hacked?" Analyzing Clinical Computer Security Interventions with Survivors of Intimate Partner Violence. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–24. https://doi.org/10.1145/3359304

[42] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2018. "A stalker's paradise": How intimate partner abusers exploit technology. *Conference on Human Factors in Computing Systems - Proceedings* 2018-April (2018), 1–13. https://doi.org/10.1145/3173574.3174241

[43] Alisa Frik, Juliann Kim, Joshua Rafael Sanchez, and Joanne Ma. 2022. Users' Expectations About and Use of Smartphone Privacy and Security Settings. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) *(CHI '22)*. Association for Computing Machinery, New

York, NY, USA, Article 407, 24 pages. https://doi.org/10.1145/3491102.3517504

[44] Christine Geeng and Franziska Roesner. 2019. *Who's In Control? Interactions In Multi-User Smart Homes.* Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3290605.3300498

[45] Douglas A. Gentile, Amy I. Nathanson, Eric E. Rasmussen, Rachel A. Reimer, and David A. Walsh. 2012. Do You See What I See? Parent and Child Reports of Parental Monitoring of Media. *Family Relations* 61, 3 (2012), 470–487. https://doi.org/10.1111/j.1741-3729.2012.00709.x

[46] Arup Kumar Ghosh, Karla Badillo-Urquiola, Shion Guha, Joseph J. Laviola, and Pamela J. Wisniewski. 2018. Safety vs. surveillance: What children have to say about mobile apps for parental control. *Conference on Human Factors in Computing Systems - Proceedings* 2018-April (2018), 1–14. https://doi.org/10.1145/3173574.3173698

[47] Arup Kumar Ghosh, Karla Badillo-Urquiola, Mary Beth Rosson, Heng Xu, John M. Carroll, and Pamela J. Wisniewski. 2018. A Matter of Control or Safety? *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* 1, CHI '18 (2018), 1–14. https://doi.org/10.1145/3173574.3173768

[48] Google. 2022. *Google Family Link.* Google. Retrieved January 31, 2022 from https://families.google.com/familylink/ Web link.

[49] Yasmeen Hashish, Andrea Bunt, and James E. Young. 2014. Involving Children in Content Control: A Collaborative and Education-Oriented Content Filtering Approach. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Toronto, Ontario, Canada) *(CHI '14)*. Association for Computing Machinery, New York, NY, USA, 1797–1806. https://doi.org/10.1145/2556288.2557128

[50] Monique M. Hedderson, Traci A. Bekelman, Mingyi Li, et al. 2023. Trends in Screen Time Use Among Children During the COVID-19 Pandemic, July 2019 Through August 2021. *JAMA Network Open* 6, 2 (2023), e2256157. https://doi.org/10.1001/jamanetworkopen.2022.56157 Accessed: 2023-08-22.

[51] J. Maya Hernandez, Elana Pearl Ben-Joseph, Stephanie M. Reich, and Linda Charmaraman. 2024. Parental Monitoring of Early Adolescent Social Technology Use in the US: A Mixed-Method Study. *Journal of Child and Family Studies* 33 (2024), 759–776. https://doi.org/10.1007/s10826-023-02734-6 Accessed: 2024-11-29.

[52] Alexis Hiniker, Sarita Y. Schoenebeck, and Julie A. Kientz. 2016. Not at the Dinner Table: Parents' and Children's Perspectives on Family Technology Rules. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work* (San Francisco, California, USA) *(CSCW '16)*. Association for Computing Machinery, New York, NY, USA, 1376–1389. https://doi.org/10.1145/2818048.2819940

[53] Anna Lena Hunkenschroer and Christoph Luetge. 2022. Ethics of AI-enabled recruiting and selection: A review and research agenda. *Journal of Business Ethics* 178, 4 (2022), 977–1007.

[54] Zainab Iftikhar, Qutaiba Rohan ul Haq, Osama Younus, Taha Sardar, Hammad Arif, Mobin Javed, and Suleman Shahid. 2021. Designing Parental Monitoring and Control Technology: A Systematic Review. In *Human-Computer Interaction–INTERACT 2021*. Springer, Online (originally Bari, Italy), 588–607.

[55] User Interviews. 2022. *User Interviews Platform.* User Interviews. Retrieved August 31, 2022 from userinterviews.com Web link.

[56] Maia Jacobs, Henriette Cramer, and Louise Barkhuus. 2016. Caring About Sharing: Couples' Practices in Single User Device Access. In *Proceedings of the 2016 ACM International Conference on Supporting Group Work* (Sanibel Island, Florida, USA) *(GROUP '16)*. Association for Computing Machinery, New York, NY, USA, 235–243. https://doi.org/10.1145/2957276.2957296

[57] Kaspersky. 2022. *Kaspersky Safe Kids.* Kaspersky Lab. Retrieved January 31, 2022 from https://usa.kaspersky.com/safe-kids Web link.

[58] Mark J Keith, Samuel C Thompson, Joanne Hale, Paul Benjamin Lowry, and Chapman Greer. 2013. Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International journal of human-computer studies* 71, 12 (2013), 1163–1173.

[59] Ada S. Kim and Katie Davis. 2017. Tweens' perspectives on their parents' media-related attitudes and rules: an exploratory study in the US. *Journal of Children and Media* 11, 3 (2017), 358–366. https://doi.org/10.1080/17482798.2017.1308399

[60] Robert S. Laufer and Max Wolfe. 1977. Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues* 33, 3 (1977), 22–42. https://doi.org/10.1111/j.1540-4560.1977.tb01880.x

[61] Jonathan Lazar, Jinjuan Heidi Feng, and Harry Hochheiser. 2017. *Research Methods in Human-Computer Interaction.* Morgan Kaufmann, Cambridge, MA, USA.

[62] NSPCC Learning. 2023. *Online risks to children: evidence review.* NSPCC Learning. https://learning.nspcc.org.uk/research-resources/2023/online-risks-to-children-evidence-review Accessed: 2023-08-22.

[63] Tama Leaver. 2017. Intimate surveillance: Normalizing parental monitoring and mediation of infants online. *Social media+ society* 3, 2 (2017), 2056305117707192.

[64] Rich Ling and Birgitte Yttri. 2012. Control, emancipation and status: The mobile telephone in the teen's parental and peer group control relationships. In *Computers, Phones and the Internet: Domesticating Information Technology.* Oxford University Press, Oxford. https://doi.org/10.1093/acprof:oso/9780195312805.003.0015

[65] MacRumors. 2024. Discussion on Apple's Ecosystem. https://www.macrumors.com. Accessed: 2024-08-26.

[66] Diogo Marques, Ildar Muslukhov, Tiago Guerreiro, Luís Carriço, and Konstantin Beznosov. 2016. Snooping on mobile phones: Prevalence and trends. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, Vol. 2. USENIX Association, USENIX Association, Berkeley, CA, 77.

[67] Tara Matthews, Kerwell Liao, Anna Turner, Marianne Berkovich, Rob Reeder, and Sunny Consolvo. 2016. "She'll just grab any device that's closer": A study of everyday device & account sharing in households. *Conference on Human Factors in Computing Systems - Proceedings* (2016), 5921–5932. https://doi.org/10.1145/2858036.2858051

[68] Dana McKay and Charlynn Miller. 2021. Standing in the Way of Control: A Call to Action to Prevent Abuse Through Better Design of Smart Technologies. In *Conference on Human Factors in Computing Systems - Proceedings.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3411764.3445114

[69] Xiaoxiao Meng and Jiaxin Liu. 2025. "Talk to me, I'm secure": investigating information disclosure to AI chatbots in the context of privacy calculus. *Online Information Review* (2025).

[70] Mobicip LLC. 2025. Mobicip Parental Control. https://www.mobicip.com/. Accessed: 2025-03-26.

[71] Jessica Morley, Luciano Floridi, Libby Kinsey, and Anat Elhalal. 2020. From what to how: an initial review of publicly available AI ethics tools, methods and research to translate principles into practices. *Science and engineering ethics* 26, 4 (2020), 2141–2168.

[72] Virginia Morrow and Martin Richards. 1996. The Ethics of Social Research with Children: An Overview. *Children & Society* 10, 2 (1996), 90–105. https://doi.org/10.1111/j.1099-0860.1996.tb00461.x

[73] Melinda Wenner Moyer. 2023. What Too Much Screen Time Does to Kids' Brains and Bodies. https://www.nytimes.com/2023/08/22/well/family/children-screen-time.html Accessed: 2023-08-22.

[74] Netnanny. 2022. *Netnanny.* ContentWatch, Inc. Retrieved January 31, 2022 from https://www.netnanny.com Web link.

[75] Helen Nissenbaum. 2004. Privacy as contextual integrity. *Wash. L. Rev.* 79 (2004), 119.

[76] Helen Nissenbaum. 2010. *Privacy in Context: Technology, Policy, and the Integrity of Social Life.* Stanford University Press, Stanford, CA.

[77] Norton. 2022. *Norton Family.* Norton. Retrieved January 31, 2022 from https://family.norton.com/web/?sr=https://www.google.com/ Web link.

[78] London School of Economics and Political Science. 2014. *Parental Controls: Advice for Parents, Researchers and Industry.* Technical Report. LSE Media Policy Project. https://core.ac.uk/download/pdf/35438359.pdf

[79] Alexandra-Mihaela Olteanu, Kévin Huguenin, Reza Shokri, Mathias Humbert, and Jean-Pierre Hubaux. 2016. Quantifying interdependent privacy risks with location data. *IEEE Transactions on Mobile Computing* 16, 3 (2016), 829–842.

[80] Our Pact. 2022. *Our Pact.* Our Pact. Retrieved August 11, 2022 from https://ourpact.com Web link.

[81] Katie N. Paulich, J. Megan Ross, Jeffrey M. Lessem, and John K. Hewitt. 2021. Screen time and early adolescent mental health, academic, and social outcomes in 9- and 10- year old children: Utilizing the Adolescent Brain Cognitive Development $^{\text{SM}}$ (ABCD) Study. *PLOS ONE* 16, 9 (09 2021), 1–23. https://doi.org/10.1371/journal.pone.0256591

[82] Pervasive Group Inc. 2025. MMGuardian Parental Control. https://www.mmguardian.com/. Accessed: 2025-03-26.

[83] Sandra Petronio. 2010. Communication privacy management theory: What do we know about family privacy regulation? *Journal of family theory & review* 2, 3 (2010), 175–196.

[84] Kruakae Pothong, Sonia Livingstone, Angela Colvert, and Larissa Pschetz. 2024. Applying children's rights to digital products: Exploring competing priorities in design. In *Proceedings of the 23rd Annual ACM Interaction Design and Children Conference* (Delft, Netherlands) *(IDC '24)*. Association for Computing Machinery, New York, NY, USA, 93–104. https://doi.org/10.1145/3628516.3655789

[85] Qustodio. 2022. *Qustodio.* Qustodio. Retrieved January 31, 2022 from https://www.qustodio.com/en/ Web link.

[86] Kopo M Ramokapane, Anthony C Mazeli, and Awais Rashid. 2019. Skip, Skip, Skip, Accept!!!: A Study on the Usability of Smartphone Manufacturer Provided Default Features and User Privacy. *Proceedings on Privacy Enhancing Technologies* 2 (2019), 209–227.

[87] Partha Pratim Ray. 2023. ChatGPT: A comprehensive review on background, applications, key challenges, bias, ethics, limitations and future scope. *Internet of Things and Cyber-Physical Systems* 3 (2023), 121–154.

[88] Michael Rich. 2023. *For kids and teens, smartphones are posing health challenges.* Harvard T.H. Chan School of Public Health. https://www.hsph.harvard.edu/news/hsph-in-the-news/for-kids-and-teens-smartphones-are-posing-health-challenges/ Accessed: 2023-08-22.

[89] Nithya Sambasivan, Garen Checkley, Amna Batool, Nova Ahmed, David Nemer, Laura Sanely Gaytán-Lugo, Tara Matthews, Sunny Consolvo, and Elizabeth Churchill. 2018. "Privacy is not for me, it's for those rich women": Performative

Privacy Practices on Mobile Phones by Women in South Asia. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. USENIX Association, Berkeley, CA, 127–142.

[90] Diane J. Schiano, Christine Burg, Anthony Nalan Smith, and Florencia Moore. 2016. Parenting Digital Youth: How Now?. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI EA '16)*. Association for Computing Machinery, New York, NY, USA, 3181–3189. https://doi.org/10.1145/2851581.2892481

[91] Eva-Maria Schomakers, Chantal Lidynia, and Martina Ziefle. 2022. The role of privacy in the acceptance of smart technologies: Applying the privacy calculus to technology acceptance. *International Journal of Human–Computer Interaction* 38, 13 (2022), 1276–1289.

[92] Varun Shiri, Maggie Xiong, Jinghui Cheng, and Jin L.C. Guo. 2024. Motivating Users to Attend to Privacy: A Theory-Driven Design Study. In *Proceedings of the 2024 ACM Designing Interactive Systems Conference* (Copenhagen, Denmark) *(DIS '24)*. Association for Computing Machinery, New York, NY, USA, 258–275. https://doi.org/10.1145/3643834.3661544

[93] Emily G. Simpson, Ashley Backman, and Christine McCauley Ohannessian. 2023. Family Functioning and Social Media Use in Early Adolescence. *Journal of Child and Family Studies* 32 (2023), 3459–3471. https://doi.org/10.1007/s10826-023-02625-w Accessed: 2024-11-29.

[94] Valerie Steeves and Owain Jones. 2010. Surveillance, children and childhood. *Surveillance & Society* 7, 3/4 (2010), 187–191.

[95] Wouter M.P. Steijn and Alexander P. Schouten. 2013. Information sharing and relationships on social networking sites. *Cyberpsychology, Behavior, and Social Networking* 16, 8 (2013), 582–587. https://doi.org/10.1089/cyber.2012.0392

[96] Magdalena Steinböck, Jakob Bleier, Mikka Rainer, Tobias Urban, Christine Utz, and Martina Lindorfer. 2024. Comparing Apples to Androids: Discovery, Retrieval, and Matching of iOS and Android Apps for Cross-Platform Analyses. In *Proceedings of the 21st International Conference on Mining Software Repositories* (Lisbon, Portugal) *(MSR '24)*. Association for Computing Machinery, New York, NY, USA, 348–360. https://doi.org/10.1145/3643991.3644896

[97] Lena H. Sun. 2023. The Negative Effects of Screen Time on Children. *The Washington Post*. https://www.washingtonpost.com/wellness/2023/09/04/toddler-screen-time-development/ Accessed: 2023-09-04.

[98] Yao Tang and Xianzhang Ning. 2023. Understanding user misrepresentation behavior on social apps: The perspective of privacy calculus theory. *Decision Support Systems* 165 (2023), 113881. https://doi.org/10.1016/j.dss.2022.113881

[99] Enterprise Apps Today. 2023. *iPhone Usage Statistics 2024 By Revenue and Users*. Enterprise Apps Today. https://www.enterpriseappstoday.com/stats/iphone-usage.html Accessed: 2024-09-05.

[100] UNICEF. 2023. *Protecting children online*. United Nations Children's Fund (UNICEF). https://www.unicef.org/protecting-children-online Accessed: 2023-08-22.

[101] Ge Wang, Jun Zhao, Samantha-Kaye Johnston, Zhilin Zhang, Max Van Kleek, and Nigel Shadbolt. 2024. CHAITok: A Proof-of-Concept System Supporting Children's Sense of Data Autonomy on Social Media. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '24)*. Association for Computing Machinery, New York, NY, USA, Article 123, 19 pages. https://doi.org/10.1145/3613904.3642294

[102] Ge Wang, Jun Zhao, Max Van Kleek, and Nigel Shadbolt. 2021. Protection or Punishment? Relating the Design Space of Parental Control Apps and Perceptions About Them to Support Parenting for Online Safety. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. ACM, Association for Computing Machinery, Online (originally Yokohama, Japan), 1–14.

[103] Tien Wang, Trong Danh Duong, and Charlie C Chen. 2016. Intention to disclose personal information via mobile applications: A privacy calculus perspective. *International journal of information management* 36, 4 (2016), 531–542.

[104] WonderShare. 2022. *FamiSafe*. WonderShare. https://famisafe.wondershare.com Accessed: August 11, 2022.

[105] Richmond Y. Wong and Deirdre K. Mulligan. 2019. Bringing Design to the Privacy Table: Broadening 'Design' in 'Privacy by Design' Through the Lens of HCI. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM, Association for Computing Machinery, Glasgow, Scotland, UK, 1–12.

[106] Richmond Y. Wong, Jason Caleb Valdez, Ashten Alexander, Ariel Chiang, Olivia Quesada, and James Pierce. 2023. Broadening Privacy and Surveillance: Eliciting Interconnected Values with a Scenarios Workbook on Smart Home Cameras. In *Proceedings of the 2023 ACM Designing Interactive Systems Conference* (Pittsburgh, PA, USA) *(DIS '23)*. Association for Computing Machinery, New York, NY, USA, 1093–1113. https://doi.org/10.1145/3563657.3596012

[107] Sarita Yardi and Amy Bruckman. 2011. Social and Technical Challenges in Parenting Teens' Social Media Use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Vancouver, BC, Canada) *(CHI '11)*. Association for Computing Machinery, New York, NY, USA, 3237–3246. https://doi.org/10.1145/1978942.1979422

[108] Leah Zhang-Kennedy, Christine Mekhail, Sonia Chiasson, and Yomna Abdelaziz. 2016. From nosy little brothers to stranger-danger: Children and parents' perception of mobile threats. In *Proceedings of IDC 2016 - The 15th International Conference on Interaction Design and Children*. ACM, New York, NY, USA, 388–399. https://doi.org/10.1145/2930674.2930716

8 Appendix

8.1 Appendix A: Screening Survey

A) Using Family Sharing Apps

1. Do you use Family Sharing on your Apple devices? (Required)

- Yes - proceed
- No - not eligible

2. How long have you used Apple's Family Sharing (in months)? *[Enter time frame in months]*

3. What are the features that you use in Apple's Family Sharing? (Please choose all that apply) (Required)

- Apple Music
- iTunes and App Store Purchases
- iCloud Storage
- Location Sharing
- Screen Time
- Apple Subscriptions
- Other, please, specify:

4. Do you use other Family Apps (for example, parental control apps, parental monitoring apps)? (please, choose all that apply)

- Microsoft Family Safety
- iSharing
- Find My Kids
- Google Family Link
- FamiSafe
- Norton Family
- FamilyTime
- Kidslox
- OurPact
- Qustodio
- Family Orbit
- Family 360
- Other, please, specify:
- I do not use other family apps

5. What are the features that you use in other family control apps? (please, choose all that apply)

- Location Tracking
- Screen Time
- Media
- Cloud Space
- Apps and Subscriptions
- Content filters
- Other, please, specify:
- I do not use other family control apps

B) Devices

6. What devices do you use Family Sharing on? (Please, choose all that apply)

- iMac
- iPad
- iPhone
- MacBook (Air, Pro)
- Apple Watch

- Other, please, specify:

7. Do your family members share these devices? [yes/no]

C) Family Structure

8. How many family members use Family Sharing?

- Less than 2 members
- 3 - 4 members
- More than 5 members

9. Do all of the family members who use Family Sharing live in the same household?

- Yes
- No

10. What is your role in your family? (Please, choose all that apply)

- Parent
- Older Sibling
- Younger Sibling
- Grandparent
- Uncle/Aunt
- Friend of the Family
- Other, please, specify:

11. What is your role in the Family Sharing App?

- Organizer
- Parent/Guardian
- Child
- Adult

Note: Demographic information were provided by the platform.

8.2 Appendix B: Interview Guide

You have been selected to participate in a research study. Participation in this study is voluntary. You can discontinue your participation in the study at any time, without needing to provide a reason. Should you discontinue your participation, you will not be subject to any negative consequences. The interview should take 40 - 45 minutes. Feel free to ask questions before, during or after the interview process.

Participants were provided a consent form, information sheet and a privacy policy. Participants were asked to read the documents carefully and sign the consent form before the interview.

A) Household arrangement, permissions, other family apps

A.1) Household arrangements

(1) How many people other than you live in your household? Could you describe the structure of your family?
  (a) What is each person's relationship to you?
(2) How are decisions made/negotiated in your family?

A.2) Permissions

(1) Does your child need to ask permission before doing activities online?

A.3) Other Family Sharing apps

(1) Have you ever used family apps other than Apple's Family Sharing app?
  (a) How would you describe them? Were they useful?
  (b) Are you still using other family apps?
  (c) Are there differences between other family apps and Apple's Family Sharing? Can you give examples?

A.4) Individual's privacy and using Family apps

(1) How do you define a child's privacy online? Could you give examples?
(2) How do you define your privacy online? Could you give examples?
  (a) What do you consider private information?
(3) What motivated you to start using Family Sharing?
(4) Can an individual's privacy be maintained when using Family Sharing? How so?
  (a) Do you have any concerns about your own privacy being affected by Family Sharing?
    (i) Do you use any techniques to maintain your own privacy?
    (ii) Do you have any concerns about sharing things accidentally?
  Do you think a child's privacy is affected by Family Sharing? How so?

B) Understanding of functionalities

B.1) Rules and regulations

(1) Are there rules in your household that Family Sharing helps you with? Could you provide examples?
  (a) What features of Family Sharing help you? Could you give examples?
  (b) How did you setup your Family Sharing app to help you with your rules?
  (c) Are there rules that Family Sharing does not help you with?

B.2) Sharing with Family

(1) What do you share with your other family members using Family Sharing? Could you give examples.
(2) What information about you can your family members see? (purchases, locations etc.)?
(3) Have you set some information to be hidden from other Family members?
  (a) Could you provide examples?
if no what do you think are the challenges with hiding information on Family Sharing?

B.3) Creating accounts and adding family members

(1) How did your child create their iCloud account?
  (a) Was the account creation done through Family Sharing?
(2) What do you think is the difference between creating an account using Family Sharing or otherwise?
  (a) Can you think of any advantages or disadvantages of creating a child's account using Family Sharing?

B.4) Devices connected to Family Sharing

(1) Do you know how many devices in your family have the Family Sharing feature turned on?
(2) How many people use the Family Sharing feature?
(3) Does your child have a device of their own? How many devices does your child use? [if not] whose device does your child use?
  (a) Do you have your own stuff on that device as well?

(b) Do you find it concerning if your child had access to adult's information? Do you use any means to protect your own privacy from your child?
(4) What does your child do on their devices?
(a) Do these devices help your child perform certain activities?
(i) What are these activities?
(5) What can you see about your child's online activity?

B.5) Features and functionalities

(1) Is there a difference between the role of an Organizer and a parent/Guardian in the context of Family Sharing? Could you explain in your own words?
(a) What is the difference between the role of a parent/Guardian and an adult?
(2) Is there a difference between the role of a child and an adult? Could you explain in your own words?
(a) A child cannot be part of two Family Sharing accounts in separate households e.g., separated partners. Why do you think that is? What do you think about this?
(3) Could you describe the process of sharing information with family members on Family Sharing?
(a) What can you share on Family Sharing? Can you give examples?
(b) What features are turn on by default? Why do you think so?
(c) What you cannot share with others on Family Sharing? Can you give examples?
(d) Is there something you want to share on Family Sharing that you are unable to?
(e) Can you share information on Family Sharing if you reside in different regions/countries? Why or why not.
(4) Who is responsible for payments in your family?
(a) Is that the same person as the organizer?
(b) Does Family Sharing store payment information? What do you think about that?
(5) Do you have Ask to Buy Permission enabled with your child?
(a) Why did you turn on this feature? What do you think about it? What does your child think about it?
(6) Do you have Screen Time Limit enabled with your child?
(a) Why did you turn on this feature? What do you think about it? What does your child think about it?
(b) What settings do you control in ScreenTime? Downtime, App limits, communication limits, apps that are always allowed, content and privacy restrictions?
(i) How do you setup these features?
(ii) What do you think about these features? Is there anything you would like to add to it?

C) Privacy Configurations of features

(1) What happens when you share iCloud storage on Family Sharing?
(2) Are you able to see what other family members are storing on their iCloud?
(3) What happens when you stop sharing on Family Sharing?
(4) How do you stop sharing Cloud storage?
(a) What happens when you stop Cloud space sharing?
(b) What happens to the information that has been previously shared?
(c) If you previously had a paid storage together on iCloud+, what happens to your files once you stop sharing Cloud space?
(d) Do you think you have been informed about this information?
(5) What do you think about sharing your location with other family members?
(a) How many family members can currently share your location?
(b) How many family members can you see their location at the moment?
(c) What happens when you disable location sharing? Is your location still shared with your device? Is this option easy to find?
(6) Do you think the Organizer has more or less privileges than an adult?
(a) What can an Organizer monitor about an adult and child accounts?
(b) Can you have more than one organizer in Family Sharing?
(c) How is an adult removed from Family Sharing?
(d) How is a child removed from Family Sharing? Is that possible?
(e) What does it mean to move families on Family Sharing?
(7) How are apps, subscriptions and purchases shared with family members?
(a) Can each member sign with their own account to the app? Do you think the organizer is able to monitor apps they have purchased?
(b) Do adults in the family need to ask before making purchases? Why do you think so?
(c) Do children need to ask before making purchases? Have you enabled this feature?
(i) What happens if the child re-installs or uses a redemption code? Would the organizer be notified?
(d) Which payment method is charged for purchases that family members make?
(e) What happens when the organizer stops sharing their payment method? (e.g., what happens to shared subscriptions like Apple TV+ and Apple Arcade).

D) Impacts of using family apps

D.1) Effects on Partner

(1) Do you think using Family Sharing can affect/affected your relationship with your partner?
(a) What are the challenges couples can face when using Family Sharing?
if yes Could you provide examples?
if yes Has anything you shared affected your relationship with your partner?
if no do you think Family Sharing can affect relationships in a positive or negative way?
(b) Has your privacy been compromised in any way? Could you give examples?

D.2) Effects on Child

(1) Do you think using Family Sharing can affect your relationship with your child? Could you provide examples?

if no What do you think are the challenges that parents-child face when using Family Sharing?

(2) How can Screen Time management affect children's experiences online? Could you provide an example? Do you think they are useful or not?

(3) Do children's views of privacy differ from their parents? (Adapted from Cranor et al. [30])

   (a) What kind of information do you think children don't want to share with their parents?

(4) Do you think that Family Sharing can have an overall positive or negative impact on families?

8.3 Appendix C: Participant Details

Table 7: Participant characteristics based on screening survey responses (occupation, age, gender, country, household income, and level of education).

#	Occupation	Age	Country	Gender	Household income	Level of education
P01	Data Analytics Analyst	40	United States	Man	$125,000 - $149,999	Postgraduate degree
P02	Manager/Assistant Manager	39	United States	Woman	$150,000 - $174,999	Undergraduate degree
P03	Business Analyst	37	United States	Man	$90,000 - $99,999	Postgraduate degree
P04	Machine Maintenance Mechanic	45	United States	Man	$200,000+	Some college
P05	Office Manager	50	United States	Woman	$100,000 - $124,999	Undergraduate degree
P06	Personal Care Worker	38	United Kingdom	Woman	$80,000 - $89,999	Undergraduate degree
P07	Registered Nurse	36	United States	Woman	$90,000 - $99,999	Undergraduate degree
P08	Consultant	49	United States	Woman	$50,000 - $59,999	Postgraduate degree
P09	Teacher/teacher Trainer	45	United Kingdom	Woman	$30,000 - $39,999	Postgraduate degree
P10	Certified Personal Trainer	35	United States	Woman	$90,000 - $99,999	Finished high school
P11	Speech Language Pathologist	35	United States	Woman	$200,000+	Postgraduate degree
P12	Manager	37	United States	Woman	$40,000 - $49,999	Postgraduate degree
P13	Chief Operating Officer	55	United States	Man	$175,000 - $199,999	Undergraduate degree
P14	Digital Director	44	United States	Man	$200,000+	Postgraduate degree
P15	Supervisor	46	United States	Man	$125,000 - $149,999	Postgraduate degree
P16	Home maker	57	United States	Woman	$100,000 - $124,999	Some college
P17	Engineering Program Manager	52	United States	Woman	$175,000 - $199,999	Undergraduate degree
P18	Teacher	44	United States	Woman	$100,000 - $124,999	Postgraduate degree
P19	Office Personnel	32	United Kingdom	Woman	$90,000 - $99,999	Undergraduate degree
P20	Critical Care Registered Nurse	36	Germany	Man	$60,000 - $69,999	Postgraduate degree

Table 8: Participant characteristics based on screening survey responses (marital status, living situation and distribution of children).

#	Marital status	Living situation	Members Using the App
P01	Married or in a civil union	With a husband/wife	Mother, Father, (2) School-aged, Grandmother, Grandfather
P02	Married or in a civil union	With a husband/wife	Mother, (3) Unknown ages*
P03	Married or in a civil union	With a husband/wife	Mother, Father, (1) Preschooler
P04	Married or in a civil union	With a husband/wife	Mother, Father, (1) Adolescent, (1) Adult
P05	Married or in a civil union	With a husband/wife	Mother, Father, (1) Adolescent, (1) Adult
P06	Married or in a civil union	With a husband/wife	Mother, Father, (4) Adolescent, (1) Toddler
P07	Divorced or separated	Undisclosed	Mother, (1) School-aged
P08	Divorced or separated	With no one	Mother, (2) School-aged
P09	Married or in a civil union	With a husband/wife	Mother, Father, (1) School-aged, (2) Adult
P10	Married or in a civil union	With a husband/wife	Mother, (1) School-aged, (1) Adolescent
P11	Married or in a civil union	With a husband/wife	Mother, Father, (2) Toddler
P12	Never married	With a significant other	Mother, Father, (1) Preschooler
P13	Married or in a civil union	With a husband/wife	Mother, Father, (1) Adolescent
P14	Divorced or separated	With no one	Mother, Grandmother, (2) School-aged
P15	Married or in a civil union	With a husband/wife	Father, (2) Adolescent
P16	Married or in a civil union	With a husband/wife	Mother, Father, (1) Adolescent
P17	Married or in a civil union	With a significant other	Mother, (1) Adolescent, (1) Adult
P18	Married or in a civil union	With a husband/wife	Mother, Father, (1) Preschooler, (1) School-aged, (1) Adolescent
P19	Married or in a civil union	With a significant other	Mother, Father, Grandmother, (1) Preschooler
P20	Married or in a civil union	With a husband/wife	Father, (1) Preschooler, (1) School-aged, (1) Adolescent

Table 9: Participant demographics based on screening survey responses: gender, marital status, living situation, education level, number of children and household income.

Demographics	N = 20	%	Demographics	N = 20	%
Gender			*Children*		
Women	13	65%	Infant (<1 year)	2	10%
Men	7	35%	Toddler (1-3 years)	2	10%
Marital Status			Preschooler (4 - 5 years)	5	25%
Married or in a civil union	16	80%	School aged (6-12 years)	8	40%
Divorced or separated	3	15%	Adolescent (13-17 years)	9	45%
Never married	1	5%	Adult (18+ years)	2	10%
Living Situation			*Household income*		
Live with a husband/wife	14	70%	$30,000 - $59,999	3	15%
Live with a significant other	3	15%	$60,000 - $69,999	1	5%
Live alone	2	10%	$80,000 - $89,999	1	5%
None of the above	1	5%	$90,000 - $99,999	4	20%
Education level			$100,000 - $124,999	3	15%
Postgraduate degree	10	50%	$125,000 - $149,999	2	10%
Undergraduate degree	7	35%	$150,000 - $174,999	1	5%
College	2	10%	$175,000 - $199,999	2	10%
Finished high school	1	5%	$200,000+	3	15%

8.4 Appendix D: Family Apps Details

Table 10: Features and platform compatability of family and parental control apps.

Family Apps	Other Features	Compatibility
Apple Family Sharing	Apple Cash for kids, Apple watch for kids, find missing device (Find My), Private Relay, Hide My Email, HomeKit Secure Video Support, usage reports.	iOS, macOS
Microsoft Family Safety	Driving Safety	iOS, Android, Windows, Xbox
iSharing	Driving safety, panic alert, location history, chat, street view.	iOS, Android
Find My Kids	Location history, listening to surroundings, SOS signal.	iOS, Android
Google Family Link	Set device bedtime, remotely lock device, see all devices where account is signed in	Android, iOS, web browsers
FamiSafe	Safe search, web history, activity report, app control.	iOS, macOS, Windows, Chromebook, Kindle, Android
Norton Family	Flags unsafe behavior online, detailed reports on kids activities, focus during remote learning, web-portal	Windows, iOS, Android (limited devices)
Family Time	Geo-fencing, safe search, block pornography, homework time.	iOS, Android
Kidslox	App blocking, location history.	iOS, Android
OurPact	View gallery, App rules, block texting, internet blocking.	iOS, Android
Qustodio	Tracks calls and SMS, Reports, Alerts and SOS.	iOS, macOS, Windows, Chromebook, Kindle, Android
Family Orbit	Text and call logger, view media, real-time alerts.	iOS, Android
Family 360	Private circle, smart notifications	iOS, Android

8.5 Appendix E: Codebook

Table 11: Codebook for the interview results (Part 1)

Theme	Code	Memo
1. Individual's Privacy	1.1 Child's Privacy	Issues related to child's privacy and experiences in the context of Family Sharing.
	1.1.1 Private	What personal information is considered private for a child.
	1.1.2 Not Private	What personal information is considered not private for a child.
	1.2 Parent's Privacy	Issues related to parents' privacy and experiences in the context of Family Sharing.
	1.2.1 Private	What personal information is considered private for a parent.
	1.2.2 Not Private	What personal information is considered not private for a parent.
	1.3 Privacy Concerns	privacy concerns in the context of Apple's Family Sharing.
	1.4 Maintaining Privacy	How users try to maintain their privacy when using Apple's Family Sharing.
2. Motivations	2.1 Reducing finances	The app allows families to save on expenses.
	2.2 Keeping in Touch	Family members can stay in touch and updated in life events with each other.
	2.3 Finding Devices	Using Find My feature to find missing devices or track family members' locations.
	2.4 Common Vendor for Devices	Apple's Family Sharing is a good option for families who share a common vendor of this ecosystem.
	2.5 Using Other Apps	Families using other parental control or collaborative family apps before, still using them or switching to Apple's Family Sharing.
	2.6 Easy to Use	The ease of use of the app as a motivation.
	2.7 Monitoring	The app offers monitoring tools for families.
3. Rules and Regulations	3.1 Making/Negotiating Decisions	Captures how decisions are made or permissions are requested and granted within the family context.
	3.2 Parenting Children	Participants discussed issues related to how they parent in this virtual spaces and what tools are particularly helpful.
	3.2.1 Access to Devices	Even with Apple's Family Sharing do parents feel they need to access their children's devices.

Table 12: Codebook for the interview results (Part 2)

Theme	Code	Memo
	3.2.2 Check location	Using the app to check locations of other members.
	3.2.3 Alternation to Parenting with Time	If parents techniques changed with the time with the updates in technology and new family apps emerging.
	3.2.4 Differences in Parenting Between Kids	If parents used different parenting techniques between kids.
	3.2.5 Permission to Buy	Concerns or processes around approving, controlling, or making purchases via shared family accounts.
4. Content Sharing	4.1 Type of content shared	Participants discussed the type of content that they share together on the app.
	4.1.1 Media	Family members using Apple's Family Sharing app to share media together.
	4.1.2 Location	Refers to the sharing and tracking of family members' locations through Family Sharing features.
	4.1.3 Apps and Subscriptions	Family members sharing apps and subscriptions together.
	4.1.4 Purchases	Family members sharing app purchases together.
	4.1.5 Cloud	Family members sharing app cloud space together.
	4.2 Sharing Accidentally	Content can be shared accidentally on the app.
	4.3 Hidden Content	Hiding or not hiding some content or personal information from other members of the app.
	4.3.1 Not Hiding Content	Content family members do not hide from each other on the app.
	4.3.2 Hiding Content	Content family members hide from each other on the app
5. Account Creation	5.1 Child creating on their own	Parent/Guardian knowledge about what it takes to create a child's account and how they did it.
	5.2 Parent Creating for Child	If the parent was the one who created the account for the child.
6. Connected Devices	6.1 Level of awareness of devices connected	The number of devices connected to the app and the parent/guardian awareness of this.
	6.2 Ownership of Child's Device	If the child owns any of the devices, or is it borrowed from the parent/guardian.

Table 13: Codebook for the interview results (Part 3)

Theme	Code	Memo
	6.2.1 Child Owner	The child owns the device.
	6.2.2 Parent Owner	The parent owns the device.
	6.3 Parent Access Child's Device	Parents access the child's device for monitoring purposes.
	6.4 Security measures of protection	What security measures are used.
	6.5 Activity on Child's Device	What activity parents track on the child's devices.
	6.5.1 Normal Activity	Parents considered the activity to be normal.
	6.5.2 Inappropriate Activity	Parents/guardians observed some inappropriate activity on their children's devices.
7. Features and Functionalities	7.1 Recognising differences in privileges	What are the extends of control that every role has on the app.
	7.1.1 Organiser-Parent/Guardian	Differences between the Organiser-Parent/Guardian roles.
	7.1.2 Parent/guardian-adult	Differences between the Parent/guardian-adult roles.
	7.1.3 Adult-Child	Differences between the Adult-child roles.
	7.2 Child part of Two Families	If the child is part of two households (e.g., separated parents).
	7.3 Process of Sharing	How families members share with each other what are their thoughts on the process.
	7.4 Members Residing in Different Locations	Family members who reside in different locations in the world and if they use the app and how.
	7.5 Role in Family Sharing	What role does the participant take on the app.
	7.5.1 Matching Role to Reality	If the role they take on the virtual app setting the same role they have in real life.
	7.5.2 Different Role than Reality	If the role they take on th virtual app setting a different role than they have in real life.
	7.6 Screen Time Restrictions	Using the app for screen time restrictions.
8. Payments	8.1 Responsible for payments	The family member responsible for the payment method or process.
	8.2 Method of Payment	Method of payment choice and issues related to apple pay, card, credit in the context of purchasing on the app.

Table 14: Codebook for the interview results (Part 4)

Theme	Code	Memo
	8.3 Storing Payment Information	Participant's thoughts about where their payment information is stored on the app.
	8.4 Security Concerns/Breaches	Concerns related to security events and threats.
	8.5 Ask to Buy	Concerns or processes around approving, controlling, or making purchases via shared family accounts.
9. Privacy Configurations	9.1 Cloud Space	How do families manage the cloud space.
	9.1.1 Effects of Disabling iCloud	What happens after disabling iCloud sharing.
	9.1.2 Informed about ata	What information is provided to users of the app when disabling enabling data sharing.
	9.2 Location Sharing	Location sharing and its functionality and configurations on the app.
	9.2.1 Effects of disabling location	What happens after users disable location sharing.
	9.2.2 Sharing location with Device	Turning on Find My on the device.
	9.3 Organizer Privileges	What can an Organizer control and do on the app.
	9.3.1 Monitoring Accounts	Monitoring other users on the app.
	9.3.2 Multiple Organizers	The idea of having multiple organizers.
	9.3.3 Removing Accounts	Removing accounts from the app and what happens to the data.
	9.3.4 Monitoring App Usage	Monitoring app usage.
	9.3.5 Members sign in to apps	Monitoring information like sign in to apps.
	9.4 Members Moving Families	Family members moving from one family to the other.
	9.5 Purchase Sharing	Family members being able to share purchases together.
	9.5.1 Effects of Disabling Payment	What happens to previously purchased apps and media when disabling payments.
	9.5.2 Notifications of Payments	Receiving notifications for payments.

Table 15: Codebook for the interview results (Part 5)

Theme	Code	Memo
10. Effects of Family Apps	10.1 Effect on couples	Effects of Apple's Family Sharing on couples.
	10.1.1 Better Communication	Improving communication.
	10.1.2 Hiding From Partner	Hiding personal information from partner.
	10.1.3 Sharing Updates About Children	Using the app to share updates about the children.
	10.1.4 Different Privileges for Parents	Parents have different privileges on the app.
	10.1.5 Trust	The effect on trust.
	10.1.6 Intrusive	The app being intrusive.
	10.1.7 Finances	Effects of the app on finances.
	10.2 Effects on Parent-Child Relation	Effect on parent-child relationship.
	10.2.1 Excessive Monitoring	Too much monitoring on the app.
	10.2.2 Better Communication	Better communication with children and parents.
	10.2.3 Locating Children	Parents/guardians being able to locate children if needed.
	10.2.4 Children Complaining	Children complaining about parenting on the app.
	10.2.5 Trust	The effect of the app on trust.
	10.3 Effect on families	The effect of Apple's Family Sharing app on families.
	10.3.1 Transparency	Communication and transparency in the app.
	10.3.2 Supervised online presence	Supervising the online activities of children.
	10.3.3 Safety	Ensuring safety using the app.
	10.3.4 Communication	Improving communication.
	10.4 Different privacy views	Participants expressed different views or opinions about data visibility, control, and privacy boundaries within the family setting.
	10.5 Children Don't Want to Share	Children not wanting to share some content.
	10.6 Effects of Screen Time	Effects of restricting screen time on children.