More Than Mere Mediators: Examining Determinants of Parental Privacy Management Behaviors

Ann-Kristin Lieberknecht
Ann-Kristin.Lieberknecht@m-chair.de
Goethe University
Frankfurt am Main, Germany

Sascha Löbner
sascha.loebner@m-chair.de
Goethe University
Frankfurt am Main, Germany

Frédéric Tronnier
frederic.tronnier@m-chair.de
Goethe University
Frankfurt am Main, Germany

Abstract

Parents face complex challenges managing children's digital privacy, navigating their own practices and multi-stakeholder family dynamics. This study develops a psychologically grounded model of parental privacy management to identify modifiable cognitive and emotional antecedents. Surveying 1,000 German parents and using structural equation modeling techniques, we examined how privacy concern and self-efficacy predict three key behaviors: child mediation, parental child data disclosure regulation, and regulation of others. Results show that privacy concern robustly predicts all three behaviors, challenging the traditional privacy paradox in parental contexts. More importantly, self-efficacy emerges as a substantially stronger predictor of privacy behaviors than concern. Among its antecedents, technical skills are most influential. Our findings suggest a paradigm shift toward peer-to-peer interventions that prioritize confidence and skill-building over fear-based approaches that emphasize privacy threats. By focusing on modifiable antecedents, this work provides practical guidance for designing interventions and platforms that empower parents to effectively protect children's privacy.

CCS Concepts

• **Security and privacy → Social aspects of security and privacy**.

Keywords

Privacy Literacy, Privacy Behavior, Parents, Children

ACM Reference Format:
Ann-Kristin Lieberknecht, Sascha Löbner, and Frédéric Tronnier. 2026. More Than Mere Mediators: Examining Determinants of Parental Privacy Management Behaviors. In *Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems (CHI '26), April 13–17, 2026, Barcelona, Spain.* ACM, New York, NY, USA, 28 pages. https://doi.org/10.1145/3772318.3790856

1 Introduction

In today's increasingly digital world, families' online activities contribute significantly to the accumulation of children's data, thereby amplifying their vulnerabilities to privacy violations. The severity of these vulnerabilities is evidenced by major regulatory actions, with Instagram (€405M, 2022) [26], TikTok (€345M, 2023) [37], and Meta (€251M, 2024) [38] sanctioned for mishandling children's data under GDPR. Additionally, studies of children's apps reveal systemic issues such as collecting or sharing personal data without consent, misusing tracking SDKs, and failing to implement privacy protections [28, 63, 77]. Against this backdrop, safeguarding children's digital privacy is not only a matter of individual vigilance but has become a pressing societal concern for researchers, policymakers, and technology developers. Central to these efforts is the recognition of parents' critical role in protecting children online [31, 41, 44, 45, 60]. Traditionally, this has been explored through the lens of parental mediation, the strategies parents use to supervise and regulate their children's online behavior to mitigate risks to privacy and safety [4, 13, 20, 21, 27, 48, 49, 61, 79].

However, this mediation-focused lens overlooks a critical dimension of family privacy: parents as privacy actors in their own right. Parents influence family privacy not only through their supervision of children's online activity but also through their own privacy-related behaviors, attitudes, and social interactions. For example, research suggests that parents may not always model the privacy-protective behaviors they expect from their children [67], and that their actions are often influenced by other stakeholders, such as friends, grandparents, and sometimes even online followers [41, 67]. These multi-stakeholder dynamics complicate how privacy is negotiated within families [4, 41].

Yet, while these dynamics are well documented, far less is known about the underlying psychological and contextual factors that shape parental privacy decisions. Without a framework that systematically examines how modifiable constructs, such as privacy concern, self-efficacy, or technical skills, translate into specific protective behaviors, researchers and practitioners remain limited in their ability to design targeted educational interventions, improve tool design, and create support systems that enhance parental privacy competence. Addressing this gap requires moving beyond descriptive accounts of parental mediation toward an explanatory model that links parents' motivations and capabilities to their concrete privacy management practices.

Building on this motivation, we investigate drivers of parental privacy management behaviors in a multi-stakeholder family context, guided by the following research questions:

RQ1: *How do parents balance privacy management behaviors, i.e. regulating their own disclosures of children's data, mediating their children's online interactions, and regulating other stakeholders, in shaping family privacy practices?*

RQ2: *What factors predict parents' privacy management behaviors within the family context?*

CHI '26, Barcelona, Spain

ACM ISBN 979-8-4007-2278-3/2026/04
https://doi.org/10.1145/3772318.3790856

RQ3: *How can insights into these behavioral predictors inform interventions and system design that better support parents in safeguarding family privacy?*

To answer these questions, we conducted a large-scale survey of 1,000 parents in Germany and applied Partial Least Squares Structural Equation Modeling (PLS-SEM) to test how internal and external factors influence parental privacy self-efficacy, privacy concern and privacy management behaviors. Our findings show that parental concern consistently predicts protective action, while self-efficacy emerges as the strongest driver of behavior, particularly when supported by technical skills.

By focusing on modifiable constructs and framing parents as privacy actors, this work makes several contributions to HCI: First, it reconceptualizes parents as active participants within multi-stakeholder networks, highlighting how family privacy emerges through interactions among children, parents, and other actors rather than solely through parental gatekeeping. Second, it identifies key modifiable predictors of parental privacy management behaviors, providing a foundation for understanding the factors that shape parents’ protective actions. Third, it demonstrates that the privacy paradox is context-dependent, showing that parental concern may result more reliably into protective behaviors in real-world family settings. Fourth, it translates these findings into practical and design-relevant insights, highlighting opportunities for interventions, educational programs, and system features that can support parents in safeguarding family privacy while reducing cognitive and social burdens.

2 Background

This section examines three interconnected areas of literature that situate parental privacy management within existing research. We first review existing work on parental concern, mediation practices, and their limitations, then explore parental privacy management behaviors, including privacy mediation as a specific subset of mediation practices, and finally examine general privacy decision-making models and their applicability to parental contexts.

2.1 Parental Concern and Mediation Practices

Parents across diverse contexts express significant concern about their children’s online safety, particularly regarding privacy [13, 20, 47, 83, 84]. Despite these concerns, many feel ill-equipped to keep pace with rapidly evolving technologies and the changing online activities of their children. These difficulties are especially evident when it comes to understanding the risks associated with the collection and sharing of personal data by online platforms and third parties [13, 20, 84]. As a result, children’s privacy protection remains fragmented and insufficient, leaving them vulnerable to various online privacy threats, including unwanted data collection or unauthorized sharing [83].

Research on how parents manage these challenges has its origins in studies of television viewing [75] and has since shifted towards the mediating of children’s internet and technology use, both from a child [25, 48, 49] and parent perspective [3, 55, 69]. Existing research has shown that parents employ a range of mediation strategies for children’s Internet use, including active mediation (sharing, encouraging, or discussing activities), restrictive mediation (rules limiting time, activities, or content), monitoring (checking usage records), and technical mediation (using software to filter or restrict access). These studies indicate that active mediation can enhance children’s engagement and understanding of online risks [48, 81], but [49] suggests it does not consistently reduce exposure to risks. In contrast, restrictive strategies, particularly rules limiting online interactions, lower some risks but can limit children’s autonomy[48, 49]. Importantly, the effectiveness of these strategies often depends on child characteristics such as age, gender, and online skills, with older or more skilled children facing greater risks regardless of mediation type [49, 55]. In practice, parents tend to favor active mediation with younger children, yet mediation decreases with age even as online risks persist [48, 49].

Several researchers have examined factors that shape parents’ engagement in parental mediation of children’s internet use. For instance, [19] find that parents who rely on expert digital security sources and possess strong digital skills engage most in active mediation. [17] show that guidance on using digital media as a parenting tool boosts parental confidence and encourages online-related conversations. Similarly, [68] demonstrate that parents’ confidence in their own smartphone skills, parenting abilities, and perceived control over mediation predicts higher levels of both active and restrictive mediation, highlighting the central role of self-efficacy. Extending this work to social video platforms, [51] show that parents’ digital literacy and confidence in understanding children’s content consumption predict mediation more strongly than perceived content risks or benefits. Their findings underscore that self-efficacy both drives mediation and shapes perceptions of risks and benefits.

2.2 Parental Privacy Management Behaviors (in a Multi-Stakeholder Family Context)

Building on this foundation, more recent studies have explored not just general parental mediation in digital contexts, but the ways in which parental approaches shape chidlrens’ and teenagers’ privacy behaviors. Parental privacy mediation represents a specialized form of parental mediation that retains the core distinction between active/instructive strategies (e.g. discussing privacy topics) and restrictive/direct interventions (e.g. configuring privacy settings), but focuses specifically on protecting children’s personal data. These practices include discussing what teens post online, reviewing their shared information, commenting on posts, reading privacy policies, and helping configure privacy settings [14, 79]. [79] found that direct intervention, such as setting privacy settings or using monitoring tools, tends to be preventive. It is associated with reduced information disclosure, smaller online networks, and lower social media use, but also with fewer opportunities for teens to develop coping strategies. In contrast, active mediation, e.g. engaging in conversations and monitoring posts without restricting actions, operates more reactively. Often applied to older teens, it is linked to greater sharing, larger networks, and more platform use, fostering autonomy and learning through corrective action. [14] similarly observed that instructive mediation, which involves discussing risks and offering guidance, predicts contact management behaviors such as blocking unknown users. Restrictive mediation, on the other hand, does not predict privacy-protective behaviors, although it does reduce information disclosure.

Despite these findings, providing effective support to parents remains a significant challenge.[83] notes a gap between parental concerns and available support, highlighting that tools addressing third-party data collection are often inaccessible and guidance for younger children is limited. Similarly, [20] emphasize the need for clear, actionable strategies to protect family privacy. Analyses of existing resources further reveal shortcomings: while most cybersecurity and educational tools target children and adolescents, very few involve parents [82], and educational features in parental control tools are rare [78].

Understanding parental privacy behavior calls for a broader view that captures how parents influence and shape digital privacy within families. In general, mediation of digital practices, parents act both as mediators of their children's online behavior and as role models through their own technology use. In the domain of online privacy, these roles are further complicated by dynamics explained in Communication Privacy Management (CPM) theory [59]. CPM theory posits that individuals establish personal and collective boundaries to manage private information within relationships. When parents share information about their child, they are not only modeling behavior but also acting as co-owners of that information, often without consciously recognizing this role. Such unawareness can result in boundary turbulence, especially as children become more invested in their own digital identities and privacy rights. Importantly, privacy boundaries in families rarely involve only the parent–child dyad. Co-parents, grandparents, extended family members, and even family friends may also be co-owners of a child's personal information, each bringing their own beliefs and expectations [41]. Differing views within this network can create mismatches in privacy norms and challenges in boundary management. [2] illustrate how this broader network can be managed through joint family oversight, where multiple family members collaboratively manage mobile privacy and security. Their findings show that including extended family can provide valuable expertise and support, but also introduce tensions. This highlights that managing children's online privacy is not simply a matter of setting rules or modeling behavior; it is embedded in a complex web of relationships and negotiations that shape family privacy practices.

Consequently, parental privacy management extends well beyond privacy mediation. It encompasses not only how parents guide and regulate their children's online practices, but also how they manage their own privacy behaviors and negotiate the actions of other stakeholders, who collectively shape a child's digital footprint. Existing studies provide valuable evidence on how parental privacy mediation influences teens' disclosure.

However, they focus primarily on mediation strategies and largely ignore parents' own privacy practices, management of other co-owners, and family dynamics, providing little insight into why parents choose to engage in such practices in the first place, beyond the general factor of privacy concern [79]. This represents a significant gap in understanding parental privacy management behaviors.

2.3 Privacy Decision-Making

Research on privacy attitudes, decision-making, and behaviors is well-established, with a central focus on the so-called "privacy paradox", the observed discrepancy between individuals' expressed valuation of privacy and their actual, often inconsistent behavior [9, 39]. This paradox has sparked interdisciplinary interest across psychology, behavioral economics, consumer marketing, and information systems. Contributions in this area vary considerably in their focus, methodology, and theoretical grounding [9, 29, 39, 70]. However, these studies are not directly transferable to the parental context. Even when variables appear conceptually similar, such as privacy concern, their meaning and implications shift. In general privacy models, privacy concern typically refers to an individual's worry about their own data being misused. In contrast, parental privacy concern involves concern for the child's data. This shift brings in fundamentally different motivations, responsibilities, and perceived consequences. Similarly, the types of privacy risks considered in parental decision-making often diverge from those that apply to adults. For example, threats likereputational damage during adolescence or long-term digital footprint implications are specific to children and teens.

One aspect of parental privacy decision-making that has received considerable attention is sharenting. Drawing on the privacy calculus model [18], studies show that parents often weigh social benefits (connection, validation, memory preservation) against privacy risks, with risks typically downplayed in practice [12, 58, 62]. Research highlights how peer influence significantly shapes sharenting behaviors, with socially more embedded parents tending to share more freely. Notably, even when parents are aware of potential consequences, this awareness rarely leads to restraint [12, 58, 62]. Beyond sharenting, work on parental control software shows that adoption is shaped by perceived risk, vulnerability, and personal innovativeness [72], while authoritarian parenting styles and teen experiences further predict use, sometimes with counterproductive outcomes [30]. While these strands of research advance our understanding of parents' privacy decision-making, they remain limited in scope.

Taken together, prior work reveals critical gaps in our understanding of parental privacy management. While existing research demonstrates how parental mediation affects teenagers [14, 79], it overlooks the underlying motivations driving parental behaviors and the complex multi-stakeholder dynamics within families. Parents must navigate not only privacy mediation, their own privacy practices but also manage information involving co-owners such as co-parents and grandparents. However, research has not yet examined how these family dynamics shape privacy decisions. This gap is particularly significant given that many parents feel overwhelmed by privacy complexities [13, 20, 84], leaving their children vulnerable to risks like unwanted data collection or unauthorized sharing [83]. Moreover, existing decision-making models, while providing a solid foundation, fail to capture the nuances of this family privacy context.

To address these gaps and inform more effective parental support systems, we conducted a large-scale (N=1,000) quantitative study with parents in Germany, employing Partial Least Squares Structural Equation Modeling (PLS-SEM) to examine parental privacy management behaviors and identify the factors shaping decisions within multi-stakeholder family contexts.

3 Research Framework

Drawing on Social Cognitive Theory (SCT) [8] and Protection Motivation Theory (PMT) [65], we propose a comprehensive model of parental privacy management. This model positions privacy concern and self-efficacy as primary drivers of protective behaviors while accounting for personal and environmental influences. Unlike existing privacy frameworks that focus solely on individual decision-making, our model captures the multilayered challenges parents face as decision-makers for their children, mediators of children's emerging privacy practices, and regulators of third-party data sharing. By focusing on modifiable factors, the framework provides pathways for educational interventions and privacy-support tool design, helping parents navigate their complex privacy management responsibilities effectively.

This section outlines the model's theoretical foundation and key constructs. It first explains how SCT and PMT jointly inform our understanding of parental privacy behaviors and provides the rationale for the variables included in the model. Building on this foundation, it then specifies the construct relationships and derives testable hypotheses, beginning with the conceptualization of the three core parental privacy management behaviors, followed by an examination of privacy concern and self-efficacy as primary drivers, along with their respective antecedents.

3.1 Theoretical Integration

We ground our model in two complementary psychological frameworks: Social Cognitive Theory (SCT) [8] and Protection Motivation Theory (PMT) [65]. SCT is a foundational theory that explains behavioral learning and regulation via observational learning, self-efficacy, and outcome expectations. These mechanisms operate within SCT's triadic reciprocal determinism, in which behavior, personal factors, and environmental influences mutually shape one another. In this study, we model the influence of personal and environmental factors on parental behavior in a single directional path, providing a clear and tractable framework while acknowledging that full reciprocal feedback loops should be explored in future research. In our model, the personal factors include both emotional and cognitive determinants, represented by Parental Privacy Concern and Perceived Parental Overload (emotional) and Parental Privacy Self-Efficacy, Parental Online Engagement, reflecting experience, Parental Privacy Knowledge, and Parental Privacy Skills (cognitive). Environmental inputs such as peer influence and children's prior victimization experiences shape these personal determinants and thereby affect subsequent behaviors.

While SCT provides a robust framework for understanding the structural determinants of parental privacy behaviors, it does not by itself explain why individuals engage in protective actions in response to perceived threats. To capture this, we integrate PMT, which explains protective responses to risk. PMT proposes that protective behaviors are motivated by two cognitive processes: 1) threat appraisal, involving assessments of vulnerability, severity, and perceived benefits of non-protective behavior, and 2) coping appraisal, involving evaluations of one's ability to respond effectively as well as response efficacy and cost. In our model, parental privacy concern and perceived vulnerability capture threat appraisal, with parental privacy concern reflecting parents' evaluation of potential privacy risks. Coping appraisal is measured with Parental Privacy Self-Efficacy.

Finally, the behavioral component of SCT and PMT is operationalized as parental privacy-management behaviors, capturing the activities parents undertake as privacy guardians for their children, including decisions about data disclosure, regulating others' access, and mediating children's emerging practices. These behaviors represent the self-regulatory outcomes emphasized in SCT and, through PMT, are understood as responses motivated by perceived threats and perceived coping ability. Importantly, the multilayered perspective makes it difficult to assess certain theory elements, such as maladaptive rewards (PMT) or action-specific response efficacy and costs (SCT), for each behavior. Nevertheless, related constructs such as perceived parental overload and susceptibility to peer influence capture incentives and barriers that may reduce protective behavior, partially accounting for perceived rewards of inaction.

By focusing on generalized threat appraisal and coping appraisal, the model identifies the key motivational mechanisms driving protective behavior while maintaining a tractable and theoretically grounded framework. It thereby contributes an overall picture of parental privacy management across multiple behaviors, guiding interventions and privacy-support tool design across diverse scenarios that are not limited to any single action.

3.2 Parental Privacy Management Behaviors as Interdependent System

According to [44], Parents engage in three interconnected privacy management behaviors that collectively shape their children's privacy landscape. First, parents make decisions about their own disclosure of children's information (*Parental Child Data Disclosure*). Second, they regulate others' sharing practices about their children (*Parental Regulation of Others*). Third, they mediate their children's developing privacy practices through education and rule-setting (*Parental Mediation Child.* We conceptualize these behaviors as mutually reinforcing components of a coherent privacy management approach. In our model, these three behaviors constitute the dependent variable, operationalizing SCT's self-regulatory outcomes and corresponding to PMT's protective behavior.

Drawing from social learning theory [6], we propose that children observe and internalize privacy norms not only from explicit instruction but also from parental modeling. We theorize that parents who demonstrate privacy-protective behaviors in their own practices may lend greater credibility and consistency to the privacy mediation they provide to their children. Conversely, we expect that contradictory behaviors, such as extensively sharing children's information while restricting children's own sharing, could potentially undermine the effectiveness of parental privacy guidance. Similarly, parents who actively regulate others' sharing about their children demonstrate a comprehensive approach to privacy protection that reinforces their mediation efforts. Additionally, parents who successfully establish privacy norms within their broader social networks may feel more confident in their ability to guide their children's privacy development. We therefore expect that parents who actively regulate others' sharing about their children will also engage more extensively in privacy mediation with their children, reflecting SCT's emphasis on the mutually reinforcing nature of self-regulatory behaviors.

H1: *Parental Child Data Disclosure* has a positive effect on *Parental Privacy Mediation.*

H2: *Parental Regulation of Others* has a positive effect on *Parental Privacy Mediation.*

3.3 Privacy Concern as Motivational Driver

PMT suggests that threat appraisal, i.e. perceived threats, vulnerabilities, and potential consequences, drives protective behaviors [65]. In the context of parental privacy management, we therefore position parental privacy concern, which reflects parents' evaluation of the seriousness of potential privacy risks, as a motivational foundation for protective action. However, we assume that the relationship between privacy concern and different types of privacy behaviors varies significantly: Research on sharenting reveals a complex relationship between parental privacy concern and disclosure behaviors. While parents often express strong concerns about potential risks to their children's privacy, they frequently continue sharing personal information [4, 41]. This apparent contradiction may result from parents' confidence in their ability to manage privacy threats, which allows them to reconcile their concerns with continued disclosure [12, 15]. Another factor may be that parents, especially of young children, often view their children as extensions of themselves rather than as independent individuals, which lowers their reluctance to disclose information on their behalf [44, 47].

Although existing literature sheds light on how privacy concerns influence parents' sharing of their children's information [12, 41, 58], research has not systematically explored how these concerns shape parents' regulation of others' sharing practices or their privacy mediation behaviors. Drawing on PMT, we propose that privacy concerns may more consistently drive such protective behaviors than they do parents' own disclosure practices. In particular, parents may perceive greater risks when privacy threats stem from others, i.e., their children, co-parents, grandparents, or third parties, reflecting a tendency to place more trust in their own ability to manage their children's information than in that of others. Therefore, we propose that while privacy concerns may not reliably restrict parents' own sharing of children's information, it may more consistently manifest in behaviors aimed at managing external privacy threats and building children's privacy capabilities.

H3a: *Parental Privacy Concern* has no significant effect on *Parental Child Data Disclosure.*

H3b: *Parental Privacy Concern* has a positive effect on *Parental Regulation of Others.*

H3c: *Parental Privacy Concern* has a positive effect on *Parental Privacy Mediation.*

Next to privacy concern, perceived vulnerability, defined as the expectation of being exposed to a threat [50], represents another key component of threat appraisal according to PMT. Empirical evidence by [22] indicates a positive relationship between perceived vulnerability to privacy risks and privacy concern. Thus, parents who believe their children are more likely to experience privacy violations may exhibit heightened concern, reflecting the activation of protective instincts in response to perceived risk. This expectation of exposure to privacy threats may be particularly salient in parental contexts, where parents' protective instincts are activated by concerns about their vulnerable dependents.

According to PMT, the threat appraisal processes can be shaped by both internal and external influences. In terms of internal influences, awareness of online threats enables individuals to recognize potential dangers more clearly and, in turn, elevates their level of concern. When knowledge is lacking, people may underestimate risks and fail to act protectively. In the parental context, educators have emphasized that many parents possess only partial knowledge of online threats [45]. External influences, such as experiences of privacy victimization, can further increase the salience of risks, making them more tangible and likely to provoke heightened vigilance and concern. Parents who have experienced privacy violations involving their children are likely to reassess vulnerability and develop stronger motivational concern for privacy protection, suggesting that concern develops not only from abstract awareness but also from lived experience [11]. Furthermore, parents who have encountered harm are likely to seek additional information about risks and protective strategies, motivated by a desire to prevent similar incidents in the future [44]. In this way, victimization functions both as a driver of concern and as a catalyst for acquiring knowledge about privacy, reinforcing parental motivation for privacy protection in PMT while also operating as an environmental influence in SCT.

Based on this reasoning, we hypothesize:

H4: *Parental Privacy Knowledge* has a positive effect on *Parental Privacy Concern.*

H5: *Perceived Vulnerability* has a positive effect on *Parental Privacy Concern.*

H6a: *Child Privacy Victimization Experience* has a positive effect on *Parental Privacy Concern.*

H6b: *Child Privacy Victimization Experience* has a positive effect on *Perceived Vulnerability.*

H6c: *Child Privacy Victimization Experience* has a positive effect on *Parental Privacy Knowledge.*

3.4 Self-Efficacy as Capability Foundation

Privacy self-efficacy, defined as an individual's belief in their ability to perform specific tasks successfully [7], is a central element of SCT's personal cognitive factors that inform self-regulatory processes, as well as of PMT's coping appraisal. It is widely recognized as a determinant of privacy behavior [16, 35]. General evidence shows that individuals with higher self-efficacy manage their disclosures more responsibly and adopt protective measures [16], though other studies could not replicate a significant link [81]. In the parental context, the evidence is similarly mixed. Some studies report that parents with higher self-efficacy are more aware of privacy risks, express greater concern, and feel more capable of using protective tools [1, 58], whereas others find no such association and suggest that confidence in managing privacy may even reduce concern if it fosters a false sense of control [62]. Beyond concern, self-efficacy has also been linked to parental mediation practices: [72] identify self-efficacy and innovativeness as predictors of parents' acceptance of parental control software, while low self-efficacy is associated with insecurity and reliance on external support [20, 44, 83].

Building on this body of work, we assume that parental self-efficacy not only affects parents' own mediation practices but also their ability to regulate others. Parents confident in their digital skills may be more likely to defend their privacy-related decisions and to restrict others' sharing of their children's information.

Therefore, we propose the following hypotheses:

- **H7a:** *Parental Privacy Self-Efficacy* has a positive effect on *Parental Child Data Disclosure.*
- **H7b:** *Parental Privacy Self-Efficacy* has a positive effect on *Parental Regulation of Others.*
- **H7c:** *Parental Privacy Self-Efficacy* has a positive effect on *Parental Privacy Mediation.*
- **H7d:** *Parental Privacy Self-Efficacy* has a positive effect on *Parental Privacy Concern.*

In line with SCT, we find evidence for several cognitive and environmental factors that influence parents' sense of competence and confidence in managing their privacy responsibilities. Among these factors, empirical research highlights technical skills as particularly central: parents with stronger technical abilities demonstrate greater awareness of how to manage privacy risks [12], whereas limited competence can undermine confidence and hinder effective use of privacy settings [45, 83]. Frequent interaction with digital tools and social media exposes parents to a broader range of features and privacy settings, further reinforcing their technical skills. In addition, privacy knowledge strengthens this process by enabling parents to recognize risks and apply strategies effectively.

At the same time, parents' privacy self-efficacy is shaped by external pressures. Social dynamics can promote sharenting: peer approval and feedback often encourage sharing behavior, thereby normalizing and reinforcing it [4]. Such reliance on social confirmation may weaken parents' confidence in their own judgment. In addition, perceived overload constrains the time and mental resources available for building skills and knowledge. As a result, parents often report a need for more time-efficient support [44], an argument supported by [83], who highlights the difficulty of explaining abstract privacy risks to parents already burdened with daily responsibilities. These external demands may indirectly reduce parents' privacy self-efficacy.

Based on this evidence, we hypothesize:

- **H8:** *Parental Susceptibility to Peer Influence* has a negative effect on *Parental Privacy Self-Efficacy.*
- **H9:** *Perceived Parental Overload* has a negative effect on *Parental Privacy Self-Efficacy.*
- **H10:** *Parental Online Engagement* has a positive effect on *Technical Privacy Skills.*
- **H11:** *Technical Privacy Skills* has a positive effect on *Parental Privacy Self-Efficacy.*
- **H12:** *Parental Privacy Knowledge* has a positive effect on *Parental Privacy Self-Efficacy.*

4 Methodology

To test our theoretical model of parental privacy management behaviors, we conducted a large-scale survey of 1,000 German parents using validated and newly developed measures. Our model conceptualizes parents as active privacy actors within the multi-stakeholder family context and focuses on three core parental privacy management behaviors: (1) parental privacy mediation of child actions, (2) parental disclosure of child data, and (3) parental regulation of other stakeholders. The model proposes that these behaviors are shaped by modifiable psychological and contextual factors. This section details our measurement instruments, data collection procedures, descriptive statistics, and analytical approach using Partial Least Squares Structural Equation Modeling (PLS-SEM) to evaluate how these factors influence parental privacy management behaviors.

4.1 Data Collection and Recruitment

The survey was administered in Germany via the professional market research institute respondi.com, which is ISO 20252 certified. Data collection took place in Oct-Nov 2024. The survey was implemented using LimeSurvey. The study was approved by the Institutional Review Board (IRB) of our institution. We did a pre-test with 50 participants. After checking the data for validity, correctness, and duration, we implemented the following changes: In the Parental Mediation section, we added the item "I restrict or prohibit my child from using websites and apps that request personal data." to capture parents' restrictive actions related to platform data collection. In the self-efficacy section, we incorporated two additional items to reflect better parents' confidence in responding to privacy threats: "I know what to do when my child's digital privacy is threatened" and "I know whom to contact when my child's digital privacy is threatened." The pre-test mean survey duration was 13.5 minutes, with a median of 8.53 minutes.

In total, 2,512 individuals participated in the survey. To ensure coverage of key developmental stages, we applied quotas based on the age of the oldest child. Quotas include 500 parents with an oldest child between 6–11 years (primary school age) and 500 parents with an oldest child between 12–15 years (early high school age). This design accounts for the assumption that parents' experiences with older children may influence how they manage the privacy of younger siblings. Within each age group, the sample was evenly balanced by gender, consisting of 250 mothers and 250 fathers. After applying the quotas, 1,360 participants were removed. Several exclusion criteria were implemented. In the beginning, we explicitly asked how many children people have. Participants answering 0 were directly excluded. Next, we asked for the age of the children. People were assigned to the aforementioned quotas (child age and parental gender) and were excluded if the respective quota was full.

To ensure quality, we used one attention check question similar to other CHI research [30]. Due to the short survey duration and the restrictive prescreening, we decided on one instructed response item [32, 53]. In compliance with the research institute, we informed participants in advance about the existence of attention questions. Furthermore, we investigated for conspicuous answering patterns, e.g., always do not know, and implausible response times [32]. Those respondents were reported to respondi.com, who compensated them and recruited new participants until 1000 were reached. We aimed for N = 1000 to have a large statistical power [23]. However, if statistical power is high, even very small effects may become statistically significant. Thus, we focus on the interpretation of meaningful path coefficients and effect sizes f^2 alongside p-values. For the multi-group PLS-SEM, we aimed for 500 participants for each group and followed the rule that group size should be at least 10 times larger than the incoming path [33]. Participants were invited until 1,000 valid cases were reached for analysis. The final average completion time was 13.2 minutes, with a median of 8.7 minutes. Table 1 summarizes the demographic characteristics and descriptive statistics of the final sample.

4.2 Descriptive Statistics

Group 1 (G1) includes 498 primary school children aged 6-11 years, and Group 2 (G2) includes 502 high school children aged 12–15. The assignment of groups was made based on the oldest child. Table 1 shows various demographics by age groups and the oldest child group (G1, G2), including the total number of children per group, gender of the oldest child, single or two-parent household, and education level of the parents. We find that the age of the parents changes in G2, with the share of 25–34 year olds declining while the share of 45–54 year olds increases, and in both groups, parents 65 and older are underrepresented. This pattern is expected, as parents age alongside their children. The average age of birth for the first child in Germany[1] is 30.1, and 31.4 overall. Thus, the mean age of 38.38 for G1 (6-11) and 42.52 for G2 (12-15) is in line with our expectations. Due to their small group size, no reliable statements can be made about age groups 18-24 and 65+. Household size is mainly two children in both groups (G1 50.4%, G2 54.8%), G2 has fewer one-child households (26.9% vs. 34.9%) and more 3+ children (18.3% vs. 14.7%). The oldest child's gender is balanced in G1 (48.4% male, 51.4% female) but skews male in G2 (66.7% male). Single or two-parent household is stable. Education skews lower overall, with slightly more highly educated parents in G2 (30.7% vs. 26.9%) and fewer medium-educated (12.9% vs. 17.5%).

4.3 Measures

4.3.1 Parental Privacy Management Behaviors. To assess parental privacy management behaviors, we distinguished three dimensions: parents' own sharing of children's data, parental mediation, and mediation of others' sharing.

Our Parental Sharing measure combines selective elements from the Parent and Child Online Engagement Scale [4] with privacy-protective strategies from [81]'s framework. From the original scale, we retained frequency of posting children's photos and sharing audience scope to directly capture core disclosure decisions about children's visual data. We excluded items that did not directly capture parents' sharing behaviors, e.g., anticipated reaction by child. To create a more comprehensive measure extending beyond photo-sharing, we incorporated the three protective strategies from [81]'s validated privacy behavior framework related to sharing personal information and adapted them to the parental context, i.e., providing false or fabricated personal information for the child and avoiding websites or apps that request children's personal data. This integration creates a more comprehensive measure of parental sharing behavior that encompasses both disclosure decisions and protection strategies across various digital contexts. All items were rated on a 5-point scale, with sharing-related items inverted to ensure consistency in measurement direction.

To capture how parents regulate the actions of others sharing their child's data, we developed a new construct: *Parental Regulation of Others*. The need for such a measure emerged from qualitative interviews with parents and media educators on privacy protection within the family conducted by [44], where a recurring theme was the difficulty parents face in asserting themselves when other stakeholders, e.g., grandparents, share information about their children. Based on these insights, we created a three-item scale measured on a 5-point Likert scale (1 = never, 5 = always). The items capture how often parents intervene when others attempt to collect data about their child without consent, when such data are posted in public online spaces, and when they are shared through private communication channels.

To assess parental strategies for regulating their children's handling of personal data online, we developed a scale grounded in prior research on parental mediation. We began with the six items from [79], who explicitly examined parental privacy mediation strategies (e.g., reading privacy policies, helping with privacy settings, using parental controls, talking about online postings). This scale was chosen as a starting point because of its strong conceptual alignment with our focus on privacy-specific mediation practices. To strengthen the measure, we incorporated four further items from [49] that cover additional aspects related to parents mediating their children's data practices. The final instrument consists of ten items, each answered on a 5-point scale (1 = never, 5 = always). At an abstract level, the items capture whether parents read privacy policies, use technical controls, help children configure privacy settings, monitor their child's data traces, talk about online disclosure practices, react to online posts, supervise data entry, review private messages, and restrict access to data-collecting platforms.

4.3.2 Internal Drivers. There exist several well established measures to assess privacy concern, like the Concern for Information Privacy (CFIP) Scale [71], Internet Users' Information Privacy Concerns (IUIPC) Scale [52], or the Internet Privacy Concerns (IPC) Scale [36], we found them to be inadequate for the purpose of our study. First, they are designed primarily for measuring individual self-concern rather than parental concern for their vulnerable dependents. Second, these scales focus predominantly on adult-oriented privacy threats, such as financial fraud, identity theft, or workplace surveillance, while overlooking the specific vulnerabilities that children face in digital environments. Therefore, we drew on [66]'s systematic literature review on cybersecurity education for children, which comprehensively mapped the landscape of digital threats specifically targeting young users. To identify child-specific privacy threats, we define them as threats arising from the exposure or misuse of children's personal information during online interactions. Though this paper focuses on privacy issues, our definition also encompasses interaction-based risks such as cyberbullying, which involves the misuse of personal information; stranger danger, which involves the disclosure or exploitation of a child's identity; and sexting, as a form of oversharing personal information. This broader framing aligns with [51], whose framework supports considering these issues together, as they arise from

[1] https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Bevoelkerung/Geburten/Tabellen/geburten-mutter-alter-bundeslaender.html (Accessed 09/01/2025)

Table 1: Group comparison across age, children, gender, household, and education

Parent age	18–24	25–34	35–44	45–54	55–64	65+	SUM	AVG
N G1 #	12	166	210	85	25	0	498	49.8%
N G2 #	5	84	225	144	41	3	502	50.2%
1 Child G1	66.7%	28.3%	28.6%	48.2%	72.0%	0.0%	174	34.9%
2 Child G1	25.0%	50.6%	59.0%	40.0%	24.0%	0.0%	251	50.4%
3+ Child G1	8.3%	21.1%	12.4%	11.8%	4.0%	0.0%	73	14.7%
1 Child G2	60.0%	13.3%	19.1%	37.5%	51.2%	100.0%	135	26.9%
2 Child G2	20.0%	61.4%	58.2%	50.7%	43.9%	0.0%	275	54.8%
3+ Child G2	20.0%	25.3%	22.7%	11.8%	4.9%	0.0%	92	18.3%
Male oldest G1	25.0%	51.2%	51.0%	45.9%	28.0%	0.0%	241	48.4%
Female oldest G1	75.0%	48.2%	49.0%	54.1%	72.0%	100.0%	256	51.4%
Male oldest G2	40.0%	69.0%	68.9%	62.5%	65.9%	100.0%	335	66.7%
Female oldest G2	60.0%	31.0%	31.1%	37.5%	34.1%	0.0%	167	33.3%
Single G1	33.3%	9.6%	11.4%	15.3%	32.0%	0.0%	65	13.1%
2 parent household G1	66.7%	90.4%	88.6%	84.7%	68.0%	0.0%	433	86.9%
Single G2	80.0%	7.1%	10.7%	17.4%	17.1%	0.0%	66	13.1%
2 parent household G2	20.0%	92.9%	89.3%	82.6%	82.9%	100.0%	436	86.9%
Education Low G1	58.3%	50.3%	56.7%	58.3%	68.0%	0.0%	276	55.4%
Education Medium G1	33.3%	25.5%	15.2%	8.3%	8.0%	0.0%	87	17.5%
Education High G1	8.3%	24.2%	28.1%	33.3%	24.0%	0.0%	134	26.9%
Education Low G2	80.0%	58.3%	51.6%	60.4%	63.4%	33.3%	283	56.4%
Education Medium G2	0.0%	23.8%	12.9%	10.4%	2.4%	0.0%	65	12.9%
Education High G2	20.0%	17.9%	35.6%	29.2%	34.1%	66.7%	154	30.7%

similar mechanisms of data exchange, interpersonal exposure, and platform-mediated interaction. Building on this conceptualization, we developed 10 questions to capture concerns that parents may experience when protecting their children's data online. In particular, parents were asked to rate the level of their concern about topics like children over-sharing information, cybergrooming, or sexting, on a 5-point scale.

Similar to privacy concerns, we found traditional scales measuring Privacy Knowledge, like the Online Privacy Literacy Scale (OPLIS) [73], inadequate for our purposes as they are centred around adult topics. Therefore, analogous to privacy concern, we developed 9 questions focusing on the different aspects of children's online privacy previously identified in [66] analysis to measure privacy concern, and asked parents to assess their knowledge on these topics on a 5-point scale.

To measure *Parental Privacy Self-efficacy*, we built upon established frameworks from [35] and [81]'s privacy self-efficacy research. Addressing the unique challenges parents face in protecting their children's digital privacy, we developed a four-item instrument that captures the multifaceted nature of parental privacy self-efficacy using a 5-point Likert scale. Directly adapting [35]'s validated approach to the parent-child context, our scale includes an assessment of parents' confidence in being able to protect children's personal data online. We also assess confidence in learning about changing online activities and associated risks, building upon [81]'s framework that emphasizes adolescents' confidence in learning skills to protect their privacy on the Internet. Additionally, our measure addresses [83] findings about parental difficulties in keeping up with developing technologies and reliance on others for support, leading us to include items measuring knowledge of appropriate responses to privacy threats and awareness of available support resources.

To the best of our knowledge, there are currently no established measurement scales that directly assess *Technical Privacy Skills*. Existing instruments instead focus more broadly on digital skills or internet-related skills [76], but they do not explicitly capture the specific competencies needed to manage children's privacy online. Given this gap, we developed our items based on the findings of [45], which draw on qualitative interviews with both parents and professional media literacy educators. These interviews revealed that many parents struggle with essential technical privacy skills, and media educators in particular observed that such limitations often hinder effective protection practices. Accordingly, our scale is grounded in these observations and practical experiences of professionals who work closely with families, rather than being adapted from an existing standardized instrument. The final scale comprises seven items measured on a 5-point Likert scale. Example items include knowing how to adjust phone settings to meet privacy expectations, install content filters to block age-inappropriate content, and configure social media settings for privacy protection.

As an antecedent of technical skills, we measured *Parental Online Engagement* based on [4]'s Parent and Child Online Engagement Scale. As a comprehensive framework for family digital interactions, we focused on three core indicators to be answered on a 5-point scale: daily internet time, social media time, and general photo posting frequency. We excluded other items of the original scale that describe contextual factors that do not directly measure parental digital usage patterns (e.g., children's social media interest) or represent outcome variables in the context of our study (e.g., sharing of children's pictures). Including these elements would have created conceptual confusion between our antecedent and dependent variables.

4.3.3 Contextual and Social Influences. *Child Privacy Victim Experience* was assessed using three items adapted from prior research on teen privacy risk-taking behavior. Specifically, we identified items from [79] that measure privacy victim experiences in teens, such as being contacted by strangers or meeting someone offline whom the child first met online. The original item wording was modified so that parents could respond about their children's experiences. Parents indicated on a 5-point scale how often their child had these experiences or reported that they did not know.

Following [35], we based the assessment of *Perceived Vulnerability* on the standard instrument by [74]. The wording was adjusted to the child context and asked parents to assess the likelihood of their children becoming victims of invasion of online privacy. We chose a single overarching item to reduce respondent burden and prevent variation in interpretation across different threats. Answers were made on a 5-point Likert scale.

Susceptibility to Peer Influence in parenting decisions was assessed using an adaptation of the well-established Susceptibility to Interpersonal Influence Scale [10]). The original scale has been widely applied in consumer and social psychology research to capture the extent to which individuals are influenced by the opinions and behaviors of others. In our study, we used three items that were measured on a 5-point Likert scale (1 = strongly disagree, 5 = strongly agree). To ensure contextual relevance, we adapted the items to the domain of parenting. The adapted items asked parents how often they seek advice from other parents when facing difficulties, whether they observe how other parents handle challenges in order to guide their own behavior, and to what extent they take into account the approval of other parents when making parenting decisions.

Recognizing that other parental obligations may significantly influence parents' capacity to engage with their children's digital privacy protection, we developed a scale to assess *Perceived Parental Overload* that impedes parental involvement in children's privacy management. This scale was developed based on insights gathered from qualitative interviews with parents and professional media literacy educators reported by [45], who emphasized the considerable burden parents face in their daily lives. Our scale conceptualizes these constraints, encompassing feelings of being overwhelmed by parental responsibilities, difficulties managing competing demands, insufficient personal time, and the cognitive burden of addressing multiple child-related concerns simultaneously. The scale consists of four items measured on a 5-point Likert scale.

4.4 Data Analysis Approach

Similar to other CHI researchers [30, 42, 56, 57], we applied structural equation modeling (SEM) to evaluate our research model. Since, to our knowledge, this study is among the first to empirically examine predictors of parental privacy management behaviors, the research is inherently exploratory. Consequently, we opted for PLS-SEM rather than CB-SEM, which is more commonly employed for theory testing [34]. The structural model was estimated using SmartPLS version 4.1.0.9 [64], with supplementary analyses conducted in SPSS. The calculations employed the path weighting scheme with a maximum of 3,000 iterations. For bootstrapping, we used the percentile bootstrap method with 5,000 subsamples. Our model comprises 12 first-order constructs, with a maximum of 4 incoming paths each. With a sample size of 498 parents with an oldest child between 6 and 11 and 502 parents with an oldest child between 12 and 15, the sample size is at least 10 times higher compared to the number of incoming paths [33]. Following Hair et al. [34], we evaluated the model using established PLS-SEM quality criteria. For reflective constructs, we investigated indicator reliability and retained items with loadings ≥ 0.7, while items between 0.4 and 0.7 were kept only when Average Variance Extracted (AVE) and Composite Reliability (CR) remained acceptable. Internal consistency was evaluated using Cronbach's α and CR, both with thresholds of ≥ 0.7 for CR. For convergent validity, we follow the recommended threshold of an AVE of at least 0.5, indicating that each construct captures more than half of the variance of its indicators. Discriminant validity was examined using the Heterotrait–Monotrait Ratio of Correlations (HTMT), which should remain below 0.85 to confirm discriminant validity. For formative constructs, we assessed multicollinearity using the Variance Inflation Factor (VIF) to ensure that values remained below 3.

5 Results

Our analysis proceeded in three stages: first evaluating the measurement model to ensure construct validity and reliability, then examining the structural model to test our hypotheses, and finally conducting multi-group analyses to explore demographic differences. In the following, we will present the respective results.

5.1 Evaluation of Measurement Model

We evaluated the outer measurement model following [34]. For all reflective constructs, reliability exceeds the 0.708 threshold, except for one item in *Perceived Parental Overload* (0.512). As internal consistency reliability, convergent validity, and discriminant validity are satisfactory for all constructs, we retain this item, consistent with [34]. The lowest reliability of internal consistency is 0.752, acceptable for exploratory research (recommended Cronbach's alpha > 0.70). The lowest AVE value is 0.559 (recommended AVE ≥ 0.50), while the highest HTMT value is 0.755 (recommended HTMT < 0.85).

For the formative constructs, all VIF values are below 3, with the highest at 2.161, indicating that there are no collinearity issues. However, for three indicators, the sign of the weight does not match the sign of the bivariate correlation with the construct. According to [34], such inconsistencies indicate potential collinearity, which can occur even at VIF values as low as 3. Therefore, these indicators are removed from the model. Among the remaining indicators, four have non-significant weights. As all of their loadings exceed the ≥ 0.50 threshold, they are retained, in accordance with the recommendations by [34].

5.2 Structural Model

5.2.1 Effects Between Parental Privacy Management Behaviors. The model revealed significant interconnections between *Parental Child Data Disclosure*, *Parental Regulation of Others*, and *Parental Mediation Child*. Specifically, *Parental Child Data Disclosure* had a strong

Table 2: Construct validity, reliability, and collinearity measures. – indicates a formative construct.

	Perceived Vulnerability	*Mediation Child*	*Mediation Others*	*Parental Child Data Disclosure*	*Parental Online Engagement*	*Past Privacy Victim Experience*	*Parental Privacy Concern*	*Parental Privacy Knowledge*	*Perceived Parental Overload*	*Parental Privacy Self Efficacy*	*Privacy Technical Skills*
N	1000	925	1000	1000	1000	986	1000	1000	1000	1000	1000
Mean	2.611	2.997	2.317	3.051	2.408	1.650	3.349	3.216	2.720	3.220	3.511
SD	0.995	0.935	1.115	0.748	0.782	0.889	0.956	0.919	1.022	0.984	0.982
Factor Loadings	1.000	0.594–	0.638–	-0.597–	0.635–	0.751–	0.800–	0.758–	0.512–	0.773–	0.732–
		0.848	0.847	0.833	0.946	0.976	0.876	0.858	0.878	0.853	0.864
CR	–	–	–	–	–	–	0.957	0.955	0.830	0.883	0.931
Cronbach's α	–	–	–	–	–	–	0.949	0.947	0.752	0.824	0.914
AVE	–	–	–	–	–	–	0.712	0.702	0.559	0.654	0.660
Min VIF	1.000	1.595	1.057	1.143	1.140	1.527	2.358	2.139	1.286	1.780	1.697
Max VIF	1.000	2.161	1.940	1.594	1.140	1.527	4.040	3.841	1.987	2.135	2.859

Table 3: Discriminant validity (HTMT values)

	Parental Privacy Concern	Parental Privacy Knowledge	Parental Privacy Self Efficacy	Perceived Parental Overload	Privacy Technical Skills	Susceptibility to Peer Influence
Parental Privacy Concern	1.0					
Parental Privacy Knowledge	0.136	1.0				
Parental Privacy Self Efficacy	0.070	0.388	1.0			
Perceived Parental Overload	0.193	0.103	0.166	1.0		
Privacy Technical Skills	0.120	0.361	0.730	0.170	1.0	
Susceptibility to Peer Influence	0.352	0.069	0.200	0.453	0.103	1.0

positive effect on *Parental Mediation Child* ($\beta = 0.395$, $t = 11.336$, $p < .000$), providing support for H1. Similarly, *Parental Regulation of Others* significantly predicted *Parental Mediation Child* ($\beta = 0.223$, $t = 5.750$, $p < .000$), supporting H2 and underscoring the interconnected nature of parental mediation strategies.

5.2.2 *Effects of Privacy Concern and Privacy Self-Efficacy.*

Parental Privacy Concern was found to significantly predict all three Parental Privacy Management Behaviors. It positively influenced *Parental Mediation Child* ($\beta = 0.169$, $t = 6.029$, $p < .001$) and *Parental Regulation of Others* ($\beta = 0.108$, $t = 3.147$, $p = .002$), supporting H3c and H3b, respectively. Contrary to H3a, *Parental Privacy Concern* also had a significant positive effect on *Parental Child Data Disclosure* ($\beta = 0.123$, $t = 3.554$, $p < .001$), indicating that higher privacy concerns are associated with greater restraint in parents' own data sharing.

Similarly, *Parental Privacy Self-Efficacy* exerted significant positive effects on all three forms of Parental Privacy Management Behaviors. It predicted *Parental Mediation Child* ($\beta = 0.223$, $t = 7.581$, $p < .001$), *Parental Regulation of Others* ($\beta = 0.188$, $t = 5.036$, $p < .001$), and *Parental Child Data Disclosure* ($\beta = 0.161$, $t = 4.732$, $p < .001$), supporting H7a, H7b, and H7c. However, *Parental Privacy Self-Efficacy* did not significantly predict *Parental Privacy Concern* ($\beta = 0.058$, $t = 1.570$, $p = .116$), resulting in no support for H7d.

5.2.3 *Antecedents of Privacy Concern.*

Several variables emerged as antecedents to *Parental Privacy Concern. Child Privacy Victim Experience* had a significant positive effect ($\beta = 0.075$, $t = 2.447$, $p = .014$), supporting H6a. However, *Parental Privacy Knowledge* only marginally predicted *Parental Privacy Concern* ($\beta = 0.074$, $t = 1.949$, $p = .051$), and did not reach conventional significance thresholds, providing no support for H4.

Moreover, *Child Privacy Victim Experience* had a significant positive effect on *Parental Privacy Knowledge* ($\beta = 0.114$, $t = 3.571$, $p < .001$), supporting H6c. Furthermore, *Child Privacy Victim Experience* had a positive effect on *Perceived Vulnerability* ($\beta = 0.364$, $t = 5.896$, $p < .001$), which in term positively affected *Parental Privacy Concern* ($\beta = 0.309$, $t = 3.912$, $p < .001$).

5.2.4 *Antecedents of Self-Efficacy.*

The strongest predictor of *Parental Privacy Self-Efficacy* was *Technical Privacy Skills* ($\beta = 0.560$, $t = 19.451$, $p < .001$), supporting H11. *Parental Privacy Knowledge* also had a significant positive effect ($\beta = 0.140$, $t = 4.702$, $p < .001$), providing support for H12. Additionally, *Parental Susceptibility to Peer Influence* had a positive effect on *Parental Privacy Self-Efficacy* ($\beta = 0.145$, $t = 6.019$, $p < .001$), contrary to H8, which posited a negative relationship. *Perceived Parental Overload* had a significant negative effect on *Parental Privacy Self-Efficacy* ($\beta = -0.109$, $t = 4.019$, $p < .001$), supporting H9. Furthermore, *Parental Online Engagement* was positively associated with *Technical Privacy Skills* ($\beta = 0.195$, $t = 6.213$, $p < .001$), supporting H10.

5.2.5 Model Summary. Overall, the model explained a substantial proportion of variance in *Parental Mediation Child* (43%), highlighting the complex and interconnected pathways among *Parental Privacy Concerns*, *Self-Efficacy*, and Parental Privacy Management Behaviors. While most hypotheses were supported (see Table 4, key exceptions included: *Parental Privacy Concern* had a positive effect on *Parental Child Data Disclosure* (contrary to H3a); *Parental Privacy Knowledge* and *Parental Privacy Self-Efficacy* did not impact *Parental Privacy Concern* (rejecting H4 and H7d); and unexpectedly, *Susceptibility to Peer Influence* positively affected *Privacy Self-Efficacy* (contrary to H8).

5.3 Control Variables

Using a two-stage approach, we found a significant moderating effect of *Age* on the relationship between *Susceptibility to Peer Influence* and *Parental Privacy Self-Efficacy* (p < .05). The simple slopes analysis showed that the effect was stronger for younger parents (path coefficient = 0.186) and weaker for older parents (path coefficient = 0.074). This indicates that privacy self-efficacy becomes less dependent on peer influence as parents get older.

Multi-group analysis revealed three significant gender differences. The effect of *Parental Online Engagement* on *Technical Privacy Skills* was stronger for males (difference = 0.190, p = 0.002), as was the effect of *Past Privacy Victim Experience* on *Perceived Vulnerability* (difference = 0.129, p = 0.016) and the effect of *Susceptibility to Peer Influence* on *Parental Privacy Self-Efficacy* (difference = 0.103, p = 0.045). Regarding single or two-parent households, there are no statistically significant differences, maybe due to the small group size of only 131 single households. Also, no significant path differences were observed between the education groups, low vs. medium and medium vs. high. The multi-group analysis between education levels low and high revealed three significant differences. The effect of *Parental Online Engagement* on *Privacy Technical Skills* was stronger among respondents with higher education (difference = 0.186, p = 0.009). Similarly, the effects of *Parental Privacy Knowledge* on *Parental Privacy Concern* (difference = 0.204, p = 0.011) and *Parental Privacy Self-Efficacy* on *Parental Privacy Concern* (difference = 0.176, p = 0.031) were stronger in the higher education group. The only robust difference between Primary School Children and High School Children lies in the effect of *Parental Privacy Self-Efficacy* on *Mediation Child*, which is significantly stronger for Primary School Children (difference = 0.152, P = 0.013).

6 Discussion

Our findings reveal several unexpected patterns in how parents approach privacy management that diverge from established models of individual privacy behavior. This section examines these patterns and their significance for theory, intervention design, and system development.

6.1 Balancing Children's Mediation, Role Modeling, and Stakeholder Navigation

In contrast to the well-established "privacy paradox," where concern rarely translates into action [9], within the context of our study, parental concern was generally linked to greater protective behaviors on all measured dimensions: *Parental Mediation Child*, *Parental Child Data Disclosures*, and *Parental Regulation of Others*. We find three possible mechanisms that explain this shift: First, most research on the privacy paradox examines individuals' concern for their own data. In the parental context, however, concern centers on children's well-being. Because children are perceived as vulnerable dependents, parents feel a strong urge to protect them [45]. This feeling may lower the risk tolerance, making concern more consistently predictive of action. Second, in the case of children, the potential consequences of privacy violations are especially vivid and emotionally powerful. Risks such as cybergrooming, sexting, or reputational harm are much more tangible than abstract concerns about targeted advertising or third-party data sharing, increasing the likelihood that concern will translate into action. Third, social comparison theory suggests that parents may evaluate their own protective behaviors in relation to those of other parents, schools, or societal norms [46, 80]. Such comparisons can lead to feelings of being judged or inadequate, thereby increasing external pressure and strengthening the incentive to translate concern into protective action. By contrast, decisions about one's own data are usually less visible to others and therefore easier to neglect. Consequently, when concerns shift from self-regarding to child-regarding, attitudes are more likely to convert into behavior. Practically, this means that awareness-raising campaigns in parental contexts may be more effective than in other domains, where concern often remains abstract and inert.

However, these findings need to be treated with caution as they contrast with previous research on sharenting, suggesting that parental concern often fails to translate into action [12]. Several factors may help explain this discrepancy. First, cultural context may be influential, since heightened privacy awareness and norms in Germany could make concern more likely to result in protective action. Second, sample characteristics may play a role, as parents in our study may have had lower baseline concern levels, which could facilitate the translation of concern into active privacy protection rather than continued sharing. Third, the broader scope of our measure *Parental Child Data Disclosure*, relative to prior work by [12], provides a more comprehensive view on parents' practices regarding children's data, although it limits strict comparability. Ultimately, our results challenge the generalizability of the privacy paradox in parental contexts, but further research is needed to determine whether this pattern holds across broader parental populations and contexts.

Concerning the different dimensions of parental privacy management behaviors, our findings reveal a systematic hierarchy: driven by privacy concern, parents most strongly engage in child privacy mediation, less so in regulating their own disclosure of children's data, and least in regulating the behaviors of others. This hierarchy may reflect the perceived urgency across these fields of action, but may also mirror the psychological ease of intervention. Direct child mediation is likely to be perceived as both a parental duty and a

Table 4: Summary of Hypothesis Testing with Effect Sizes (f^2)

Hyp.	Path	p-value	Path Coeff.	f^2	Decision
H1	Parental Child Data Disclosure → Parental Privacy Mediation	0.000	0.395	0.006	accept
H2	Parental Regulation of Others → Parental Privacy Mediation	0.006	0.223	0.013	accept
H3a	Parental Privacy Concern → Parental Child Data Disclosure	0.091	0.123	0.153	reject
H3b	Parental Privacy Concern → Parental Regulation of Others	0.131	0.108	0.229	reject
H3c	Parental Privacy Concern → Parental Privacy Mediation	0.004	0.169	0.039	accept
H4	Parental Privacy Knowledge → Parental Privacy Concern	0.308	0.082	0.007	reject
H5	Perceived Vulnerability → Parental Privacy Concern	0.000	0.309	0.094	accept
H6a	Child Privacy Victimization Experience → Parental Privacy Concern	0.203	0.075	0.006	reject
H6b	Child Privacy Victimization Experience → Perceived Vulnerability	0.000	0.364	0.153	accept
H6c	Child Privacy Victimization Experience → Parental Privacy Knowledge	0.103	0.114	0.013	reject
H7a	Parental Privacy Self-Efficacy → Parental Child Data Disclosure	0.029	0.161	0.027	accept
H7b	Parental Privacy Self-Efficacy → Parental Regulation of Others	0.016	0.188	0.037	accept
H7c	Parental Privacy Self-Efficacy → Parental Privacy Mediation	0.000	0.223	0.083	accept
H7d	Parental Privacy Self-Efficacy → Parental Privacy Concern	0.488	0.057	0.003	reject
H8	Parental Susceptibility to Peer Influence → Parental Privacy Self-Efficacy	0.005	0.145	0.033	reject*
H9	Perceived Parental Overload → Parental Privacy Self-Efficacy	0.061	-0.109	0.019	reject*
H10	Parental Online Engagement → Technical Privacy Skills	0.003	0.195	0.039	accept
H11	Technical Privacy Skills → Parental Privacy Self-Efficacy	0.000	0.560	0.485	accept
H12	Parental Privacy Knowledge → Parental Privacy Self-Efficacy	0.021	0.140	0.031	accept

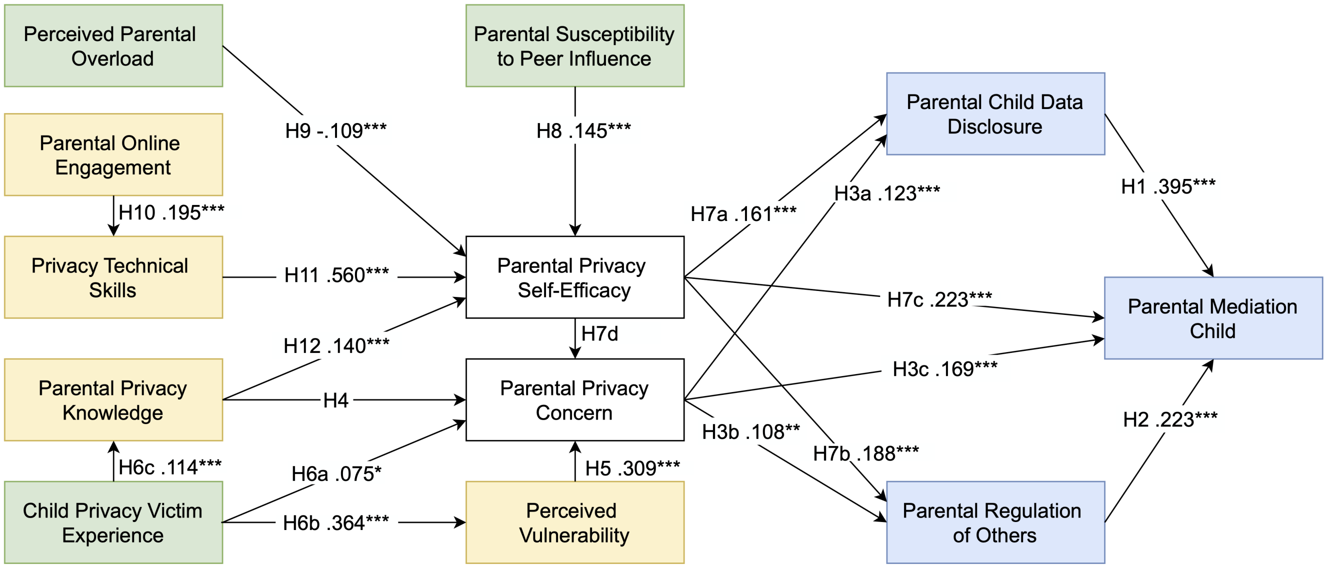

Figure 1: Structural Equation Model. Yellow nodes represent internal factors, green nodes external factors, and blue nodes parental privacy management behaviors. Arrows indicate hypothesized relationships tested, with path coefficients showing the strength of the relationships. Significance levels are indicated as follows: $p < 0.05$ (*), $p < 0.01$ (**), and $p < 0.001$ (***).

domain of authority. By contrast, regulating their own disclosure requires parents to acknowledge their role-modeling responsibilities, which may be psychologically uncomfortable and less salient in everyday practice [67]. Moreover, parents may perceive their own disclosures as safer, given that these are intentional and under their control, in line with findings of [12, 15], whereas the actions of others are less predictable. The comparatively weakest effect was observed for regulating others, which may be explained by the relational costs and social discomfort associated with confrontation, found by [44]. These findings suggest that privacy protection is shaped not only by cognitive processes but also by relational and emotional negotiations embedded in broader family and social dynamics.

Further evidence for the multi-stakeholder nature of parental privacy management comes from the significant influence of regulating others on child mediation. This indicates that protecting children's privacy is not limited to a parent–child dyad but involves coordination across social networks, including grandparents, co-parents, schools, and peers. According to CPM theory, each of these actors has their own privacy norms and behaviors, creating a complex landscape of co-ownership over children's digital information [59]. The distributed responsibility of parents to not only mediate their children's actions but also police broader networks can contribute to parents' perceived overload and may generate relational tension, as boundary turbulence arises not only when children resist rules but also when extended family members or other stakeholders disregard parental expectations. These findings highlight the need for interventions and tools that support parents in navigating multi-stakeholder privacy environments.

6.2 Reflecting Predictors of Parental Privacy Management Behaviors

While *Parental Privacy Concern* was consistently predictive, *Parental Privacy Self-efficacy* emerged as the stronger driver of protective behaviors. This finding aligns with SCT [8], stating that confidence in one's ability to act increases the likelihood of actual behavior. It also highlights the limitations of fear-based approaches: raising concern without equipping parents with practical skills risks generating anxiety without translating into action. This is in line with findings by [24] who showed that fear appeals may boost short-term compliance but also generate negative emotions, while self-efficacy fosters more enduring security practices.

A similar pattern is reflected in [68], who recommend providing parents with education, guidelines, and practical tools to enhance their confidence and effectiveness in mediating children's smartphone use, with actionable strategies supporting both active and restrictive mediation. Recent work on social video platforms further reinforces this point: [51] find that parents' confidence and digital literacy outweigh perceived harms in predicting whether they intervene, suggesting that self-efficacy not only increases mediation but also shapes how parents evaluate competing risks and benefits on online platforms.

Notably, unlike *Parental Privacy Concern*, *Parental Self-efficacy* had a relatively stronger effect on the *Regulation of Others* than on *Parental Child Data Disclosures*. We propose two potential explanations. First, in line with prior research, parents with higher self-efficacy may feel confident in managing data disclosures responsibly (e.g., by using appropriate privacy settings) and therefore, may share more of their children's data [12, 15], which could weaken the effect on parental disclosure. Second, parents with high self-efficacy may feel more confident in confronting others, a task that is likely to be perceived as socially uncomfortable or challenging.

A central, though unsurprising, finding is that *Technical Privacy Skills* predicts *Parental Privacy Self-efficacy* substantially more strongly than *Parental Privacy Knowledge*. Thus, theoretical knowledge on privacy risks is less effective for building self-efficacy than procedural knowledge on how to act, i.e., how to adjust privacy settings, set filters, or manage permissions. This implies that interventions should prioritize hands-on, skills-based learning rather than abstract information campaigns, a conclusion supported by [54], who found that youths with high privacy knowledge often had high concern but lower protective behavior due to optimism bias, highlighting the importance of actionable, procedural skills over abstract knowledge.

A more unexpected finding is that *Susceptibility to Peer Influence* enhanced, rather than diminished, *Parental Privacy Self-efficacy*. Rather than undermining confidence, peer networks appear to function as social learning environments, where observing, exchanging, and validating practices increases perceived competence. The findings suggest that social comparison can play a positive pedagogical role in privacy management: parents may learn from each other, normalize protective practices, and gain reassurance. This claim is backed up by prior research, which similarly recommends peer-to-peer and community-based learning for parents, emphasizing that parents value the opinions and experiences of other parents and are motivated by interaction with them [45]. Designing peer-to-peer-based, community-centered interventions may therefore be more effective than purely individualistic training programs.

Considering the control variables, education significantly amplified how online engagement translated into technical skills and how knowledge shaped concern and efficacy. Unsurprisingly, higher education appears to function as a cognitive amplifier, enabling parents to convert experiences into skills and to integrate abstract knowledge into effective attitudes. These findings highlight the importance of providing clear, practical guidance to support parents with lower formal education in developing skills and confidence for effective digital privacy management.

Furthermore, our findings revealed a significant gender disparity in *Technical Privacy Skills*, with mothers reporting lower levels compared to fathers. Given that *Technical Privacy Skills* is the strongest predictor of *Parental Privacy Self-efficacy*, which in turn drives privacy management behaviors, this gender gap has important implications for family privacy protection. This pattern may be particularly relevant in more traditional families where mothers take on a larger share of mediating children's digital activities. The result is a potential disconnect: those parents who are most likely to be involved in day-to-day privacy decisions and attending information sessions about digital privacy may simultaneously demonstrate lower technical confidence. This aligns with prior findings showing that while mothers are more often engaged in monitoring children's devices, they frequently defer technical tasks such as setting parental controls or managing software permissions to fathers, reflecting enduring gender stereotypes in technology use [19, 61]. Therefore, one possible way forward could be to explore gender-sensitive interventions that provide mothers with practical technical skills, thereby strengthening their role as mediators of family privacy. Thus, empowering these parents technically could have a disproportionate impact on the overall quality of family privacy practices.

Finally, *Parental Privacy Self-efficacy* was most predictive when children were in primary school rather than early secondary school, suggesting that parents' confidence plays a particularly important role when children are younger and more dependent. This may reflect that, as children grow older and assert greater autonomy, parental control tends to diminish and mediation becomes less direct. These findings reinforce calls for parents to establish a strong media relationship with their child early on, while guidance is both more feasible and more impactful [45, 83].

Contextualizing our findings within the broader parental mediation literature, our results suggest that privacy mediation shares important similarities with parental mediation of children's online interactions. Consistent with the broader mediation literature, parental skills, self-efficacy, and knowledge are important predictors of privacy mediation practices. This aligns with and extends existing research on parental mediation of internet usage [17, 19], smartphone usage [68], and video games [51]. In our study, we further found that privacy concern drives privacy mediation practices. This contrasts with prior qualitative research, which showed that even parents who expressed high concern for their children's privacy did not necessarily select privacy-friendly apps [83]. These differing findings can be explained by different methodologies. While [83] examined actual behavior, our study relied on self-reported behavior. We also examined a broader range of privacy mediation practices, not only usage restrictions. Notably, our model validation procedures revealed no anomalies; consequently, participants behaved consistently with this strategy relative to others.

Nevertheless, the observation by [83] points to a critical distinction between privacy mediation and general online mediation: Differentiating privacy-invasive from privacy-friendly apps is a highly specific task requiring substantial expertise. Compared to the general supervision of internet usage, privacy mediation often demands considerably more technical skills and specialized knowledge. This technical barrier is particularly concerning given earlier noted gender disparities in privacy technical skills. Furthermore, our analysis shows that privacy mediation does not operate in isolation but rather forms part of a larger constellation of privacy management behaviors. These dimensions are highly interconnected and emotionally intertwined. They reflect parents' multifaceted roles not merely as role models and gatekeepers of their children's behavior, but as co-owners of their children's personal information who bear responsibility for boundary management in their own disclosure practices and for regulating other co-owners such as extended family members.

Against this backdrop, it is important to recognize that parental mediation is not a monolithic construct. Although treating privacy mediation as a unified measure allowed us to situate it within broader parental privacy-management behaviors and maintain model stability, prior research shows that different mediation strategies can be shaped by distinct antecedents. Higher digital skills and parental self-efficacy are typically associated with active, conversation-based mediation [17, 19], whereas restrictive, rule-based practices often emerge from heightened perceptions of risk [43]. Consequently, the antecedents identified in our study may relate differently to specific privacy mediation strategies. Future research should therefore differentiate among these strategies to clarify whether privacy-specific mediation aligns with, or departs from, the broader parental mediation framework.

6.3 Informing Interventions and System Design

Our findings reveal several promising directions for intervention design and platform development. While grounded in observed patterns, these implications require validation through real-world testing to confirm their practical feasibility and effectiveness. This is particularly important since our model relies on self-reported behavior, which may be subject to bias and may not fully capture actual parental practices. Against this backdrop, we outline five key principles intended to strengthen the design and effectiveness of future interventions:

(1) Approaches that strengthen parents' sense of efficacy may be more effective than fear-based messaging, given that self-efficacy emerged as a stronger predictor of protective behavior than concern alone. This suggests that interventions should prioritize capability-building rather than threat awareness.
(2) Procedural knowledge proves more valuable than abstract information, with parents benefiting more from hands-on training than theoretical instruction. This indicates that practical, actionable guidance yields better outcomes than conceptual understanding alone.
(3) Peer networks offer valuable resources for knowledge sharing and support, suggesting that community-centered learning approaches may be more effective than individual-focused interventions.
(4) Observed differences in technical skills between mothers and fathers highlight the need for inclusive, gender-sensitive interventions. These interventions should address distinct needs and build technical confidence among caregivers underserved by traditional technology education, ensuring both mothers and fathers are equally supported.
(5) The moderating role of educational level indicates that programs must accommodate varying levels of digital literacy to reach their intended audiences effectively.

Our findings further highlight two content-focused areas that may warrant particular attention. First, helping parents critically reflect on their own disclosure practices could raise awareness of their role-modeling function for children, which in turn strongly influences how they approach parental privacy mediation. This self-reflection may improve consistency between parents' privacy expectations for their children and their own sharing behaviors. Second, providing concrete strategies for managing third-party disclosures, such as negotiation techniques with relatives or co-parents, may strengthen parents' confidence when handling sensitive situations that extend beyond their direct control. Additionally, extending privacy education to broader networks, including grandparents, schools, and peer groups, could further help address the inherently multi-stakeholder character of children's digital privacy. This aligns with previous research that highlights that strong partnerships with trusted intermediaries, such as schools or educators, can enhance parent engagement and effectively bridge gaps in knowledge [17], making privacy guidance more actionable and impactful. Complementing this perspective, [40] emphasize the importance of community and peer-based support in managing digital privacy and security, showing that trusted social networks, including friends, family, and co-workers, can collectively enhance privacy efficacy and provide informal guidance through tech caregiving.

The study highlights practical opportunities for digital platforms to reduce parental burden by supporting privacy management across multiple stakeholders. Cross-stakeholder privacy tools could enable parents to enforce privacy preferences across accounts and devices used by co-parents, relatives, or other caregivers, ensuring consistent application of rules even outside the immediate household. Customizable family group features could help parents manage privacy within the household by organizing children, siblings, or relatives into groups, allowing default sharing rules to apply automatically and eliminating the need to adjust settings individually. As highlighted by [40], this kind of community-based privacy support can enhance privacy efficacy by sharing guidance, normalizing collaborative privacy practices, and possibly sustaining engagement over time. Platforms could also support negotiating third-party disclosures, such as when relatives, friends, or co-parents want to share content involving a child. The system could prompt them to request parental approval before posting, and once confirmed, content would be automatically shared according to the parent's preferences. Additionally, platforms could provide mechanisms that allow parents to request that shared content be removed or adjusted without fear of relational costs or social discomfort, through guided prompts, templated messages, or private notifications. Together, these features offer tangible, actionable design directions that reflect the networked, multi-actor nature of children's digital footprints and reduce parental effort while maintaining control over family privacy, echoing the recommendations of [2].

6.4 Limitations and Future Work

This study offers a holistic framing of parents as privacy actors, expanding beyond the traditional child-centered perspective to consider not only parental mediation of children's digital behaviors but also parents' own privacy practices and their roles within multi-stakeholder family contexts. Drawing on a large-scale quantitative study with 1,000 parents in Germany, we employed Partial Least Squares Structural Equation Modeling (PLS-SEM) to empirically identify and analyze the factors that shape different parental privacy management behaviors, including *Parental Privacy Self-efficacy*, *Parental Privacy Concern*, *Technical Privacy Skills*, and broader contextual variables. Our findings advance HCI privacy theory in several ways. In particular, the work contributes by demonstrating that the so-called "privacy paradox" is context-dependent: in parental settings, concern may translate into protective behavior more reliably. Furthermore, it shifts the perspective of parents from gatekeepers to privacy actors embedded within multi-stakeholder networks. Empirically, it provides the first large-scale model of modifiable predictors that shape parental privacy management behaviors. Practically, these findings suggest that interventions should prioritize capability-building over fear appeals, incorporate hands-on training, support gender-sensitive skill development, and leverage peer and community networks. From a design perspective, the results point to opportunities for systems that reduce parental burden through cross-stakeholder privacy tools, family group settings, and support for negotiating third-party disclosures.

Several limitations should be considered when interpreting these results. We relied on self-reported behaviors rather than observed actions, which may be influenced by social desirability. Similarly, privacy technical skills and privacy knowledge were self-assessed and may not accurately reflect actual abilities or understanding. We did not measure how parental mediation translates into child outcomes, such as behavior, knowledge, or self-efficacy. Furthermore, our model simplifies the theoretical mechanisms by representing personal and environmental influences on parental behavior as a single directional path. This approach provides a focused framework that highlights key drivers of parental privacy behaviors, though it does not capture the full reciprocal feedback loops emphasized by SCT. Similarly, adopting a multilayered perspective on parental privacy management behaviors enabled us to examine a broad range of actions and motivations across contexts, while limiting the assessment of certain theory elements, such as maladaptive rewards (PMT) or action-specific response efficacy and costs (SCT), pointing to clear avenues for future research. In addition, we treated parental mediation as a single construct rather than differentiating between strategies (i.e. active mediation, restrictive mediation). Collapsing them into a unified construct allowed us to preserve model stability and focus on broader parental privacy management tendencies. Future research should disentangle these strategies to examine whether different antecedents differentially shape specific forms of mediation.

Although our model explained 43% of the variance in parental mediation, which is substantial for exploratory research, it also highlights that other factors are likely to be at play. While we focused on modifiable constructs, future research could examine how personality types, parenting styles, such as authoritarian, permissive, or autonomy-supportive approaches, shape the strategies parents use to manage privacy. Children's own agency, including their compliance, resistance, and emerging privacy skills, may further influence how parental guidance translates into behavior. Moreover, because digital platforms differ in their affordances and constraints, contextual studies are needed to understand how these variations facilitate or hinder parental regulation. Since our sample was limited to Germany, replication in other cultural settings is also necessary to account for differences in parenting norms and privacy expectations. Finally, because our study did not test interventions directly, the practical feasibility of the proposed design implications remains to be validated in real-world settings.

Taken together, these limitations and directions for future research underscore the complexity of parental privacy management and highlight the need for continued investigation into theoretical models, practical interventions, and system designs that support parents in multi-stakeholder digital environments.

7 Conclusion

This study is the first to investigate the drivers of parental privacy management behaviors, examining not only how parents mediate their children's digital activities but also how they manage their own privacy and navigate multi-stakeholder family contexts. We found that parental concern consistently translated into protective behaviors across multiple domains, challenging the generalizability of the privacy paradox and highlighting that, in parental contexts, concern may lead to action more reliably. Self-efficacy emerged as a particularly strong predictor, emphasizing the central role of confidence and perceived capability in shaping protective behaviors. These findings point to several promising directions for supporting parents. Interventions and digital platforms may benefit from focusing on strengthening parental confidence, providing practical guidance, and leveraging social networks, while also accounting for diverse family contexts, gender roles, and levels of digital literacy. Ultimately, this work underscores that protecting children's privacy online depends on recognizing and supporting parents as empowered actors within complex digital and social systems.

Acknowledgments

The authors would like to acknowledge financial support through the project CyberSecPro funded by the European Union's DIGITAL-2021-SKILLS-01 Programme under grant agreement no. 101083594. Furthermore, this research work is also a contribution to the International Alliance for Strengthening Cybersecurity and Privacy in Healthcare (CybAlliance, Project no. 337316).

References

[1] Kishalay Adhikari and Rajeev Kumar Panda. 2018. Users' Information Privacy Concerns and Privacy Protection Behaviors in Social Networks. *Journal of Global Marketing* 31, 2 (March 2018), 96–110. doi:10.1080/08911762.2017.1412552 Publisher: Routledge.

[2] Mamtaj Akter, Leena Alghamdi, Jess Kropczynski, Heather Richter Lipford, and Pamela J. Wisniewski. 2023. It Takes a Village: A Case for Including Extended Family Members in the Joint Oversight of Family-based Privacy and Security for Mobile Smartphones. In *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems (CHI EA '23)*. Association for Computing Machinery, New York, NY, USA, 1–7. doi:10.1145/3544549.3585904

[3] Rabia Üstündağ Alkan, Alper Aslan, Yiğit Emrah Turgut, and Engin Kurşun. 2021. Factors Affecting Parental Mediation Strategies in Children's Technology Use: A Systematic Review. *Journal of Computer and Education Research* 9, 18 (Dec. 2021), 702–723. doi:10.18009/jcer.925859 Publisher: Tamer KUTLUCA.

[4] Mary Jean Amon, Nika Kartvelishvili, Bennett I. Bertenthal, Kurt Hugenberg, and Apu Kapadia. 2022. Sharenting and Children's Privacy in the United States: Parenting Style, Practices, and Perspectives on Sharing Young Children's Photos on Social Media. *Proc. ACM Hum.-Comput. Interact.* 6, CSCW1 (April 2022). doi:10.1145/3512963 Place: New York, NY, USA Publisher: Association for Computing Machinery.

[5] Young Min Baek, Eun-mee Kim, and Young Bae. 2014. My privacy is okay, but theirs is endangered: Why comparative optimism matters in online privacy concerns. *Computers in Human Behavior* 31 (Feb. 2014), 48–56. doi:10.1016/j.chb.2013.10.010

[6] Albert Bandura. 1977. *Social Learning Theory*. Prentice Hall. Google-Books-ID: IXvuAAAAMAAJ.

[7] Albert Bandura. 1978. Self-efficacy: Toward a unifying theory of behavioral change. *Advances in Behaviour Research and Therapy* 1, 4 (Jan. 1978), 139–161. doi:10.1016/0146-6402(78)90002-4

[8] Albert Bandura. 1986. *Social foundations of thought and action: A social cognitive theory*. Prentice-Hall, Inc, Englewood Cliffs, NJ, US. Pages: xiii, 617.

[9] Susanne Barth and Menno D. T. de Jong. 2017. The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics* 34, 7 (Nov. 2017), 1038–1058. doi:10.1016/j.tele.2017.04.013

[10] William O. Bearden, Richard G. Netemeyer, and Jesse E. Teel. 1989. Measurement of Consumer Susceptibility to Interpersonal Influence. *Journal of Consumer Research* 15, 4 (March 1989), 473–481. doi:10.1086/209186

[11] France Belanger and Robert E. Crossler. 2019. Dealing with digital traces: Understanding protective behaviors on mobile devices. *The Journal of Strategic Information Systems* 28, 1 (March 2019), 34–49. doi:10.1016/j.jsis.2018.11.002

[12] Niamh Ní Bhroin, Thuy Dinh, Kira Thiel, Germany Hans-Bredow-Institut, Claudia Lampert, Germany Hans-Bredow-Institut, Elisabeth Staksrud, and Kjartan Ólafsson. 2022. The Privacy Paradox by Proxy: Considering Predictors of Sharenting. *Media and Communication* 10, 1 (2022), 371–383. doi:10.17645/mac.v10i1.4858 Publisher: Cogitatio Press.

[13] Rita Brito and Patrícia Dias. 2020. "Which apps are good for my children?": How the parents of young children select apps. *International Journal of Child-Computer Interaction* 26 (2020), 100188. ISBN: 2212-8689 Publisher: Elsevier.

[14] Hongliang Chen, Christopher E. Beaudoin, and Traci Hong. 2016. Teen online information disclosure: Empirical testing of a protection motivation and social capital model. *Journal of the Association for Information Science & Technology* 67, 12 (Dec. 2016), 2871–2881. http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=119478020&lang=de&site=ehost-live

[15] Hsuan-Ting Chen. 2018. Revisiting the Privacy Paradox on Social Media With an Extended Privacy Calculus Model: The Effect of Privacy Concerns, Privacy Self-Efficacy, and Social Capital on Privacy Management. *American Behavioral Scientist* 62, 10 (Sept. 2018), 1392–1412. doi:10.1177/0002764218792691 Publisher: SAGE Publications Inc.

[16] Hsuan-Ting Chen and Wenhong Chen. 2015. Couldn't or Wouldn't? The Influence of Privacy Concerns and Self-Efficacy in Privacy Management on Privacy Protection. *Cyberpsychology, Behavior, and Social Networking* 18, 1 (Jan. 2015), 13–19. doi:10.1089/cyber.2014.0456 Publisher: Mary Ann Liebert, Inc., publishers.

[17] Anne Clarkson and Lori Zierl. 2018. An Online Parenting Program Grows Digital Parenting Skills and Parent–School Connection. *The Journal of Extension* 56, 5 (Sept. 2018). doi:10.34068/joe.56.05.06

[18] Mary J. Culnan and Pamela K. Armstrong. 1999. Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science* 10, 1 (Feb. 1999), 104–115. doi:10.1287/orsc.10.1.104 Publisher: INFORMS.

[19] Lenka Dedkova, David Smahel, and Mike Just. 2022. Digital security in families: the sources of information relate to the active mediation of internet safety and parental internet skills. *Behaviour & Information Technology* 41, 5 (April 2022), 1052–1064. doi:10.1080/0144929X.2020.1851769 Publisher: Taylor & Francis.

[20] Laurien Desimpelaere, Liselot Hudders, and Dieneke Van de Sompel. 2020. Children's and Parents' Perceptions of Online Commercial Data Practices: A Qualitative Study. *Media and Communication* 8, 4 (Nov. 2020), 163–174. doi:10.17645/mac.v8i4.3232 Number: 4.

[21] Patrícia Dias and Rita Brito. 2019. How families with young children are solving the dilemma between privacy and protection by building trust - a portrait from portugal. *Journal of Children and Media* (Nov. 2019). doi:10.1080/17482798.2019.1694552 Publisher: Taylor & Francis.

[22] Tamara Dinev and Paul Hart. 2004. Internet privacy concerns and their antecedents - measurement validity and a regression model. *Behaviour & Information Technology* 23, 6 (Dec. 2004), 413–422. http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=14794972&lang=de&site=ehost-live

[23] Nicola Döring and Jürgen Bortz. 2016. *Forschungsmethoden und evaluation*. Vol. 5. Springer.

[24] Marc Dupuis, Karen Renaud, and Anna Jennings. 2022. Fear might motivate secure password choices in the short term, but at what cost?. In *Proceedings of the Hawaii International Conference on System Sciences (HICSS)*. University of Strathclyde, Glasgow, Scotland. https://strathprints.strath.ac.uk/77671/ Accepted Author Manuscript.

[25] Matthew S. Eastin, Bradley S. Greenberg, and Linda Hofschire. 2006. Parenting the Internet. *Journal of Communication* 56, 3 (Sept. 2006), 486–504. doi:10.1111/j.1460-2466.2006.00297.x

[26] European Data Protection Board. 2022. Record fine for Instagram following EDPB intervention. Press release. https://www.edpb.europa.eu/news/news/2022/record-fine-instagram-following-edpb-intervention_en

[27] Lorleen Farrugia and Mary Anne Lauri. 2018. Maltese parents' awareness and management of risks their children face online. Nordicom, University of Gothenburg, 135–146. http://urn.kb.se/resolve?urn=urn:nbn:se:norden:org:diva-12026

[28] Álvaro Feal, Paolo Calciati, Narseo Vallina-Rodriguez, Carmela Troncoso, and Alessandra Gorla. 2020. Angel or Devil? A Privacy Study of Mobile Parental Control Apps. In *Proceedings of Privacy Enhancing Technologies (PoPETS)*, Vol. 2020. Montreal, Canada. https://eprints.networks.imdea.org/2080/

[29] Nina Gerber, Paul Gerber, and Melanie Volkamer. 2018. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security* 77 (Aug. 2018), 226–261. doi:10.1016/j.cose.2018.04.002

[30] 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? Examining Parental Use of Technical Monitoring Apps on Teens' Mobile Devices. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. Association for Computing Machinery, New York, NY, USA, 1–14. doi:10.1145/3173574.3173768

[31] Moritz Gruber, Christian Höfig, Maximilian Golla, Tobias Urban, and Matteo Große-Kampmann. 2022. "We may share the number of diaper changes": A Privacy and Security Analysis of Mobile Child Care Applications.

[32] Tobias Gummer, Joss Roßmann, and Henning Silber. 2021. Using instructed response items as attention checks in web surveys: Properties and implementation. *Sociological Methods & Research* 50, 1 (2021), 238–264.

[33] Joseph F Hair. 2014. *A primer on partial least squares structural equation modeling (PLS-SEM)*. sage.

[34] Joseph F Hair Jr, G Tomas M Hult, Christian M Ringle, Marko Sarstedt, Nicholas P Danks, and Soumya Ray. 2021. *Partial least squares structural equation modeling (PLS-SEM) using R: A workbook*. Springer Nature.

[35] Cho Hichang. 2010. Determinants of Behavioral Responses to Online Privacy: The Effects of Concern, Risk Beliefs, Self-Efficacy, and Communication Sources on Self-Protection Strategies. *Journal of Information Privacy and Security* 6, 1 (Jan. 2010), 3–27. doi:10.1080/15536548.2010.10855879 Publisher: Routledge.

[36] Weiyin Hong and James Y. L. Thong. 2013. INTERNET PRIVACY CONCERNS: AN INTEGRATED CONCEPTUALIZATION AND FOUR EMPIRICAL STUDIES. *MIS Quarterly* 37, 1 (March 2013), 275–298. http://search.ebscohost.com/login.

aspx?direct=true&db=buh&AN=85634464&lang=de&site=ehost-live

[37] Irish Data Protection Commission. 2023. Irish Data Protection Commission announces €345 million fine of TikTok. Press release. https://www.dataprotection.ie/en/news-media/press-releases/DPC-announces-345-million-euro-fine-of-TikTok

[38] Irish Data Protection Commission. 2024. Irish Data Protection Commission fines Meta €251 million. Press release. https://www.dataprotection.ie/en/news-media/press-releases/irish-data-protection-commission-fines-meta-eu251-million

[39] Spyros Kokolakis. 2017. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security* 64 (Jan. 2017), 122–134. doi:10.1016/j.cose.2015.07.002

[40] Jess Kropczynski, Reza Ghaiumy Anaraky, Mamtaj Akter, Amy J. Godfrey, Heather Lipford, and Pamela J. Wisniewski. 2021. Examining Collaborative Support for Privacy and Security in the Broader Context of Tech Caregiving. *Proc. ACM Hum.-Comput. Interact.* 5, CSCW2 (Oct. 2021), 396:1–396:23. doi:10.1145/3479540

[41] Priya Kumar and Sarita Schoenebeck. 2015. The modern day baby book: Enacting good mothering and stewarding privacy on Facebook. In *Proceedings of the 18th ACM conference on computer supported cooperative work & social computing*. 1302–1312.

[42] Heejae Lee, Gabriel Dominguez Partida, Nicholas David Bowman, and Philippe de Villemor Chauveau. 2025. Translation and Validation of The Video Game Demand Scale to Spanish. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems (CHI '25)*. Association for Computing Machinery, New York, NY, USA, Article 339, 14 pages. doi:10.1145/3706598.3713216

[43] Sook-Jung Lee. 2013. Parental restrictive mediation of children's internet use: Effective for what and for whom? *New Media & Society* 15, 4 (June 2013), 466–481. doi:10.1177/1461444812452412 Publisher: SAGE Publications.

[44] Ann-Kristin Lieberknecht. 2024. Exploring Determinants of Parental Engagement in Online Privacy Protection: A Qualitative Approach. In *Proceedings of the 2024 European Symposium on Usable Security (EuroUSEC '24)*. Association for Computing Machinery, New York, NY, USA, 94–111. doi:10.1145/3688459.3688476

[45] Ann-Kristin Lieberknecht and Aline Melanie Ochs. 2024. Safeguarding Children's Digital Privacy: Exploring Design Requirements for Effective Literacy Training for Parents. In *Information Security Education - Challenges in the Digital Age*, Lynette Drevin, Wai Sze Leung, and Suné von Solms (Eds.). Springer Nature Switzerland, Cham, 111–126. doi:10.1007/978-3-031-62918-1_8

[46] Hongyang Liu, Jana Kvintova, and Lucie Vachova. 2025. Parents' social comparisons and adolescent self-esteem: the mediating effect of upward social comparison and the moderating influence of optimism. *Frontiers in Psychology* 16 (January 2025), 1473318. doi:10.3389/fpsyg.2025.1473318

[47] Sonia Livingstone and Jasmina Byrne. 2018. Parenting in the Digital Age. The Challenges of Parental Responsibility in Comparative Perspective. In *Digital parenting: the challenges for families in the digital age*, Giovanna Mascheroni, Cristina Ponte, and Ana Jorge (Eds.). Nordicom, Göteborg, 19–30.

[48] Sonia Livingstone, Leslie Haddon, Anke Görzig, and Kjartan Ólafsson. 2011. Risks and safety on the internet: the perspective of European children: full findings and policy implications from the EU Kids Online survey of 9-16 year olds and their parents in 25 countries. http://www.eukidsonline.net/ Num Pages: 159 Place: London, UK Publisher: EU Kids Online, The London School of Economics and Political Science.

[49] Sonia Livingstone and Ellen J. Helsper. 2008. Parental Mediation of Children's Internet Use. *Journal of Broadcasting & Electronic Media* 52, 4 (Nov. 2008), 581–599. doi:10.1080/08838150802437396 Publisher: Routledge.

[50] May O. Lwin and Seang-Mei Saw. 2007. Protecting Children from Myopia: A PMT Perspective for Improving Health Marketing Communications. *Journal of Health Communication* 12, 3 (May 2007), 251–268. doi:10.1080/10810730701266299 Publisher: Taylor & Francis.

[51] Renkai Ma, Yao Li, Sunhye Bai, Yubo Kou, and Xinning Gui. 2025. Weighing Benefits and Harms: Parental Mediation on Social Video Platforms. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems (CHI '25)*. Association for Computing Machinery, New York, NY, USA, 1–26. doi:10.1145/3706598.3713422

[52] Naresh K. Malhotra, Sung S. Kim, and James Agarwal. 2004. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research* 15, 4 (Dec. 2004), 336–355. http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=15648475&lang=de&site=ehost-live

[53] Adam W Meade and S Bartholomew Craig. 2012. Identifying careless responses in survey data. *Psychological methods* 17, 3 (2012), 437.

[54] Xiaoyang Meng and Bobo Feng. 2022. Online taxi users' optimistic bias: China youths' digital travel and information privacy protection. *Frontiers in Psychology* 13 (2022), 1049925. doi:10.3389/fpsyg.2022.1049925

[55] Peter Nikken and Marjon Schols. 2015. How and Why Parents Guide the Media Use of Young Children. *Journal of Child and Family Studies* 24, 11 (2015), 3423–3435. doi:10.1007/s10826-015-0144-4

[56] Rita Orji, Regan L. Mandryk, and Julita Vassileva. 2017. Improving the Efficacy of Games for Change Using Personalization Models. *ACM Trans. Comput.-Hum. Interact.* 24, 5, Article 32 (Oct. 2017), 22 pages. doi:10.1145/3119929

[57] Rita Orji, Gustavo F Tondello, and Lennart E Nacke. 2018. Personalizing persuasive strategies in gameful systems to gamification user types. In *Proceedings of the 2018 CHI conference on human factors in computing systems*. 1–14.

[58] Zhao Peng. 2024. A privacy calculus model perspective that explains why parents sharent. *Information, Communication & Society* 27, 11 (Aug. 2024), 2129–2152. doi:10.1080/1369118X.2023.2285462 Publisher: Routledge.

[59] Sandra Petronio. 2002. *Boundaries of Privacy: Dialectics of Disclosure.* SUNY Press. Google-Books-ID: gTCsft8zVXgC.

[60] Farzana Quayyum. 2023. Collaboration between parents and children to raise cybersecurity awareness. In *European Interdisciplinary Cybersecurity Conference.* ACM, Stavanger Norway, 149–152. doi:10.1145/3590777.3590802

[61] Farzana Quayyum and Letizia Jaccheri. 2023. *An exploratory study about the role of gender in cybersecurity awareness for children.* IADIS Press. https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/3103888 Accepted: 2023-11-21T14:05:30Z Journal Abbreviation: An exploratory study about the role of gender in cybersecurity awareness for children Publication Title: 73-80.

[62] Giulia Ranzini, Gemma Newlands, and Christoph Lutz. 2020. Sharenting, Peer Influence, and Privacy Concerns: A Study on the Instagram-Sharing Behaviors of Parents in the United Kingdom. *Social Media + Society* 6, 4 (Oct. 2020), 2056305120978376. doi:10.1177/2056305120978376 Publisher: SAGE Publications Ltd.

[63] Irwin Reyes, Primal Wijesekera, Joel Reardon, Amit Elazari Bar On, Abbas Razaghpanah, Narseo Vallina-Rodriguez, and Serge Egelman. 2018. "Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale. Barcelona, Spain. https://eprints.networks.imdea.org/1795/

[64] Christian M. Ringle, Sven Wende, and Jan-Michael Becker. 2024. *SmartPLS 4*. SmartPLS, Bönningstedt. https://www.smartpls.com

[65] R Rogers, John Cacioppo, and Richard Petty. 1983. Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. 153–177.

[66] Rahime Belen Sağlam, Vincent Miller, and Virginia N. L. Franqueira. 2023. A Systematic Literature Review on Cyber Security Education for Children. *IEEE Transactions on Education* 66, 3 (June 2023), 274–286. doi:10.1109/TE.2022.3231019

[67] Gisela Schubert and Susanne Eggert. 2018. "Daddy, Your Mobile is Stupid, you should Put it Away". Media Education from the Perspective of Professionals in Brazil. Reflecting a Broader "Macho" Culture. In *Digital parenting: the challenges for families in the digital age*, Giovanna Mascheroni, Cristina Ponte, and Ana Jorge (Eds.). Nordicom, Göteborg, 147–156.

[68] Wonsun Shin. 2018. Empowered parents: the role of self-efficacy in parental mediation of children's smartphone use in the United States. *Journal of Children and Media* 12, 4 (Oct. 2018), 465–477. doi:10.1080/17482798.2018.1486331 Publisher: Routledge.

[69] Wonsun Shin and Hye Kyung Kim. 2019. What Motivates Parents to Mediate Children's Use of Smartphones? An Application of the Theory of Planned Behavior. *Journal of Broadcasting & Electronic Media* 63, 1 (Jan. 2019), 144–159. doi:10.1080/08838151.2019.1576263 Publisher: Routledge.

[70] Yefim Shulman. 2018. Towards a Broadening of Privacy Decision-Making Models: The Use of Cognitive Architectures. In *Privacy and Identity Management. The Smart Revolution*, Marit Hansen, Eleni Kosta, Igor Nai-Fovino, and Simone Fischer-Hübner (Eds.). Vol. 526. Springer International Publishing, Cham, 187–204. doi:10.1007/978-3-319-92925-5_12 Series Title: IFIP Advances in Information and Communication Technology.

[71] H. Jeff Smith, Sandra J. Milberg, and Sandra J. Burke. 1996. Information Privacy: Measuring Individuals' Concerns About Organizational Practices. *MIS Quarterly* 20, 2 (June 1996), 167–196. http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=9610124512&lang=de&site=ehost-live

[72] Kristin Stewart, Glen Brodowsky, and Donald Sciglimpaglia. 2021. Parental supervision and control of adolescents' problematic internet use: understanding and predicting adoption of parental control software. *Young Consumers: Insight and Ideas for Responsible Marketers* 23, 2 (Sept. 2021), 213–232. doi:10.1108/YC-04-2021-1307

[73] Sabine Trepte, Doris Teutsch, Philipp K. Masur, Carolin Eicher, Mona Fischer, Alisa Hennhöfer, and Fabienne Lind. 2015. Do People Know About Privacy and Data Protection Strategies? Towards the "Online Privacy Literacy Scale" (OPLIS). In *Reforming European Data Protection Law*, Serge Gutwirth, Ronald Leenes, and Paul de Hert (Eds.). Springer Netherlands, Dordrecht, 333–365. doi:10.1007/978-94-017-9385-8_14

[74] Tom R. Tyler. 1980. Impact of directly and indirectly experienced events: The origin of crime-related judgments and behaviors. *Journal of Personality and Social Psychology* 39, 1 (1980), 13–28. doi:10.1037/0022-3514.39.1.13 Place: US Publisher: American Psychological Association.

[75] Patti M. Valkenburg, Marina Krcmar, Allerd L. Peeters, and Nies M. Marseille. 1999. Developing a scale to assess three styles of television mediation: "Instructive mediation," "restrictive mediation," and "social coviewing". *Journal of Broadcasting & Electronic Media* 43, 1 (Jan. 1999), 52–66. doi:10.1080/08838159909364474 Publisher: Routledge.

[76] Alexander J.A.M. van Deursen, Ellen J. Helsper, and Rebecca Eynon. 2016. Development and validation of the Internet Skills Scale (ISS). *Information, Communication & Society* 19, 6 (June 2016), 804–823. doi:10.1080/1369118X.2015.1078834 Publisher: Routledge.

[77] Natalija Vlajic, Marmara El Masri, Gianluigi M. Riva, Marguerite Barry, and Derek Doran. 2018. Online Tracking of Kids and Teens by Means of Invisible Images: COPPA vs. GDPR. In *Proceedings of the 2nd International Workshop on Multimedia Privacy and Security (MPS '18)*. Association for Computing Machinery, New York, NY, USA, 96–103. doi:10.1145/3267357.3267370

[78] Pamela Wisniewski, Arup Kumar Ghosh, Heng Xu, Mary Beth Rosson, and John M. Carroll. 2017. Parental Control vs. Teen Self-Regulation: Is there a middle ground for mobile online safety?. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW '17)*. Association for Computing Machinery, New York, NY, USA, 51–69. doi:10.1145/2998181.2998352

[79] Pamela Wisniewski, Haiyan Jia, Heng Xu, Mary Beth Rosson, and John M. Carroll. 2015. "Preventative" vs. "Reactive": How Parental Mediation Influences Teens' Social Media Privacy Behaviors. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing (CSCW '15)*. Association for Computing Machinery, New York, NY, USA, 302–316. doi:10.1145/2675133.2675293 event-place: Vancouver, BC, Canada.

[80] Qiuyue Yang, Jianjun Gu, and Jon-Chao Hong. 2021. Parental Social Comparison Related to Tutoring Anxiety, and Guided Approaches to Assisting Their Children's Home Online Learning During the COVID-19 Lockdown. *Frontiers in Psychology* 12 (July 2021), 708221. doi:10.3389/fpsyg.2021.708221

[81] Seounmi Youn. 2009. Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents. *Journal of Consumer Affairs* 43, 3 (2009), 389–418. doi:10.1111/j.1745-6606.2009.01146.x

[82] Leah Zhang-Kennedy and Sonia Chiasson. 2021. A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education. *Comput. Surveys* 54, 1 (Jan. 2021), 12:1–12:39. doi:10.1145/3427920

[83] Jun Zhao. 2018. Are Children Well-Supported by Their Parents Concerning Online Privacy Risks, and Who Supports the Parents? doi:10.48550/arXiv.1809.10944 arXiv:1809.10944 [cs].

[84] Jun Zhao, Ulrik Lyngs, and Nigel Shadbolt. 2018. What privacy concerns do parents have about children's mobile apps, and how can they stay SHARP? doi:10.48550/arXiv.1809.10841 arXiv:1809.10841 [cs].

A Appendix: Constructs (German)

	Question	Item	Ref.
PPK	Wie gut schätzen Sie Ihr Wissen über folgende Themen ein?	Übermäßiges Teilen von persönlichen Informationen	[66]
		Identitätsdiebstahl und -betrug	
		Profiling und Tracking	
		Sexting (Senden oder Empfangen von sexuellen Inhalten	
		Cyber-Grooming (sexuelle Ansprache online durch Fremde	
		Kontaktaufnahme durch Fremde	
		Missbräuchliche Verwendung von Daten	
		Digitale Überwachung	
		Cybermobbing	
PPC	Ich bin besorgt...	...um die digitalen Privatsphäre meines Kindes.	[66]
		...darüber, dass mein Kind übermäßig persönlichen Informationen über sich teilt.	
		...d., dass die Identität meines Kindes online geklaut wird und damit kriminelle Handlungen ausgeführt werden.	
		...darüber, dass mein Kind online getrackt wird und ein Profil über mein Kind angelegt wird.	
		...darüber, dass mein Kind Sexting (Austausch erotischer Texte, Fotos, Videos) betreibt.	
		...darüber, dass mein Kind online sexuell angesprochen wird.	
		...darüber, dass Fremde mein Kind online kontaktieren.	
		...dass Informationen über mein Kindes im Internet missbräuchlich verwendet werden.	
		...dass mein Kind digital überwacht wird.	
		...dass mein Kind Opfer von Cybermobbing wird.	
CPV	Wie wahrscheinlich ist es, ...	Mein Kind hat Dinge online gepostet/geteilt, die es später bereut hat.	[79]
		Mein Kind hat sich mit jemandem physisch getroffen, den es online kennengelernt hat.	
		Mein Kind wurde online von Fremden kontaktiert.	
PEV	Wie wahrscheinlich ist es, ...	...dass ihr Kind Opfer einer missbräuchlichen Verwendung von persönlichen Daten wird?	[5]
POE	Bitte beantworten Sie die folgenden Fragen.	Wie viel Zeit verbringen Sie täglich im Internet?	[4]
		Wie viel Zeit verbringen Sie täglich auf Sozialen Medien?	
		Wie häufig posten Sie Fotos online?	
PSE	Wie sehr stimmen Sie den folgenden Aussagen zu?	Ich bin zuversichtlich, dass ich die persönlichen Daten meines Kindes online schützen kann.	[81]
		Ich bin zuversichtlich, dass ich mich mit den sich verändernden Online-Aktivitäten meines Kindes und den daraus resultierenden Gefahren auf dem Laufenden halten kann.	[35]
		Ich weiß, was ich tun muss, wenn die digitale Privatsphäre meines Kindes bedroht ist.	[83]
		Ich weiß, an wen ich mich wenden kann, wenn die digitale Privatsphäre meines Kindes bedroht ist.	[84]
TPS	Wie sehr stimmen Sie den folgenden Aussagen zu? Ich weiß, wie man die folgenden Maßnahmen durchführt:	Einstellungen auf dem Handy anpassen, sodass sie meinen Vorstellungen von Privatsphäre-Schutz entsprechen.	[44]
		Handy-Einstellungen anpassen, um Einkäufe und Downloads auf dem Handy (duch mein Kind) zu verhindern.	
		Handy-Einstellungen anpassen, um Zeitbegrenzungen für Apps einzurichten.	
		Auf dem Handy Inhaltsfilter installieren, die nicht altersgerechte Inhalte wegfiltern.	
		App-Berechtigungen anpassen, sodass sie meinen Vorstellungen von Privatsphäre-Schutz entsprechen.	
		Einstellungen auf Social-Media anpassen, sodass sie meinen Vorstellungen von Privatsphäre-Schutz entsprechen.	
		Ein Browser-Plugin installieren, welches Werbe- und Tracking Cookies blockiert.	
PPO	Wie sehr stimmen Sie den folgenden Aussagen über Ihre Rolle als Eltern zu?	Ich fühle mich von den Anforderungen und der Verantwortung, die ich als Elternteil zu tragen habe, überfordert.	[44]
		Es fällt mir schwer, mit den vielfältigen Aufgaben und Verpflichtungen als Elternteil zu jonglieren.	
		Als Elternteil habe ich zu wenig Zeit für mich selbst.	
		Als Elternteil habe ich viele Sorgen und Themen (z. B. Schulnoten, gesunde Ernährung usw.), um die ich mich kümmern muss.	
PSP	Wie sehr stimmen Sie den folgenden Aussagen hinsichtlich anderen Eltern zu?	Ich wende mich oft an andere Eltern, um den besten Weg im Umgang mit den Problemen meines Kindes zu finden.	[10]
		Um sicherzugehen, dass ich mich richtig verhalte, beobachte ich oft, wie andere Eltern mit Problemen umgehen.	
		Wenn ich Erziehungsentscheidungen treffe, entscheide ich in der Regel so wie ich denke, dass andere Eltern es gut finden.	
PCD	Bitte beantworten Sie die folgenden Fragen.	Wie häufig teilen/posten Sie Fotos von Ihrem Kind auf Sozialen Medien?	[4]
		Mit wem teilen Sie Fotos von Ihrem Kind auf Sozialen Medien?	
		Ich verwende online einen falschen Namen oder einen falschen Ausweis für mein Kind.	[81]
		Ich gebe online unvollständige Informationen über mein Kind an.	[81]
		Ich greife auf andere Websites/Apps zurück, die nicht nach den persönlichen Daten meines Kindes fragen.	
PRO	Bitte beantworten Sie die folgenden Fragen.	Wenn jemand, den ich nicht kenne, ein Foto von meinem Kind machen möchte, bitte ich ihn, dies nicht zu tun.	[44]
		Wie oft erheben Sie Einwände dagegen, dass Andere Fotos von Ihrem Kind auf Sozialen Medien posten?	
		Wie oft erheben Sie Einwände dagegen, dass Andere Fotos von Ihrem Kind auf Messengern teilen?	
PMC	Wie oft treffen Sie die folgenden Maßnahmen, wenn Ihr Kind online ist?	Ich lese vor der Nutzung einer Website oder App durch mein Kind die Datenschutzrichtlinien.	[79]
		Ich verwende Kindersicherungen, um die Online-Aktivitäten meines Kindes zu blockieren, zu filtern oder zu überwachen.	
		Ich helfe meinem Kind beim Einrichten der Datenschutzeinstellungen.	
		Ich suche online nach den Daten meines Kindes.	
		Ich spreche mit meinem Kind über meine Bedenken bezüglich seiner Online-Postings.	
		Ich kommentiere oder antworte direkt auf die Online-Postings meines Kindes.	
		Ich sitze bei meinem Kind, wenn es persönliche Daten angibt.	
		Ich kontrolliere die persönlichen Nachrichten meines Kindes.	[49]
		Ich schränke ein/verbiete meinem Kind die Nutzung von Webseiten und Apps, die persönliche Daten abfragen.	

Construct Abbreviations: PPK = Parental Privacy Knowledge; PPC = Parental Privacy Concern; CPV = Child Privacy Victimization Experience; PEV = Perceived Vulnerability; POE = Parental Online Engagement; PSE = Parental Privacy Self-Efficacy; TPS = Technical Privacy Skills; PPO = Perceived Parental Overload; PSP = Parental Susceptibility to Peer Influence; PCD = Parental Child Data Disclosure; PRO = Parental Regulation of Others; PMC = Parental Privacy Mediation Child.

B Appendix: Constructs (Translated into English)

	Question	Item	Ref.
PPK	How well do you assess your knowledge on the following topics?	Oversharing of personal information	[66]
		Identity theft and fraud	
		Profiling and tracking	
		Sexting (sending or receiving sexual content)	
		Cyber-grooming (sexual approaches online by strangers)	
		Contact by strangers	
		Misuse of data	
		Digital surveillance	
		Cyberbullying	
PPC	I am concerned...	...about my child's digital privacy.	[66]
		...that my child shares too much personal information.	
		...that my child's identity is stolen online and used for criminal activities.	
		...that my child is tracked online and a profile is created about them.	
		...that my child engages in sexting (exchange of erotic texts, photos, videos).	
		...that my child is approached sexually online.	
		...that strangers contact my child online.	
		...that information about my child is misused on the internet.	
		...that my child is digitally monitored.	
		...that my child becomes a victim of cyberbullying.	
CPV	Which activities has your child engaged in?	My child has posted/shared things online that they later regretted.	[79]
		My child has met someone in person whom they first met online.	
		My child has been contacted online by strangers.	
PEV	How likely is it that ...	...your child will fall victim to improper use of personal information?	[5]
		...other children will fall victim to improper use of personal information?	
POE	Please answer the following questions.	How much time do you spend online each day?	[4]
		How much time do you spend on social media each day?	
		How often do you post photos online?	
PSE	To what extent do you agree with the following statements?	I am confident that I can protect my child's personal data online.	[81]
		I am confident that I can keep up with my child's evolving online activities and the risks that arise from them.	[35]
		I know what to do when my child's digital privacy is threatened.	[83]
		I know whom to contact when my child's digital privacy is threatened.	[84]
TPS	I know how to perform the following actions:	Adjust smartphone settings so that they align with my privacy preferences.	[44]
		Adjust smartphone settings to prevent purchases and downloads (by my child).	
		Adjust smartphone settings to set time limits for apps.	
		Install content filters on the smartphone that block age-inappropriate content.	
		Adjust app permissions so that they align with my privacy preferences.	
		Adjust privacy settings on social media platforms to match my privacy preferences.	
		Install a browser plugin that blocks advertising and tracking cookies.	
PPO	To what extent do you agree with the following statements?	I feel overwhelmed by the demands and responsibilities I carry as a parent.	[44]
		I find it difficult to juggle the various tasks and obligations associated with being a parent.	
		As a parent, I have too little time for myself.	
		As a parent, I have many concerns and issues to deal with (e.g., school grades, healthy nutrition).	
PSP	To what extent do you agree with the following statements?	I often turn to other parents to find the best way to handle my child's problems.	[10]
		To make sure I am doing the right thing, I often observe how other parents deal with problems.	
		When making parenting decisions, I usually choose what I think other parents would approve of.	
PCD	Please answer the following questions.	How often do you share/post photos of your child on social media?	[4]
		With whom do you share photos of your child on social media?	
		I use a false name or false identity for my child online.	[81]
		I provide incomplete information about my child online.	
		I use websites/apps that do not ask for personal data about my child.	
PRO	Please answer the following questions.	If someone I don't know wants to take a photo of my child, I ask them not to do so.	[44]
		How often do you object when others post photos of your child on social media?	
		How often do you object when others share photos of your child on messengers?	
PMC	How often do you take the following actions when your child is online?	I read the privacy policies of a website or app before my child uses it.	[79]
		I use parental controls to block, filter, or monitor my child's online activities.	
		I help my child configure privacy settings.	
		I search online for information about my child.	
		I talk with my child about my concerns regarding their online postings.	
		I comment on or directly respond to my child's online posts.	
		I sit next to my child when they enter personal information online.	[49]
		I check my child's private messages.	
		I restrict or prohibit my child from using websites or apps that request personal data.	

Construct Abbreviations: PPK = Parental Privacy Knowledge; PPC = Parental Privacy Concern; CPV = Child Privacy Victimization Experience; PEV = Perceived Vulnerability; POE = Parental Online Engagement; PSE = Parental Privacy Self-Efficacy; TPS = Technical Privacy Skills; PPO = Perceived Parental Overload; PSP = Parental Susceptibility to Peer Influence; PCD = Parental Child Data Disclosure; PRO = Parental Regulation of Others; PMC = Parental Privacy Mediation Child.

C Survey (German)

C.1 Demografische Daten 1/2

Wie alt sind Sie?

[unter 18; 18; 19; ...; 75; älter 75]

Bitte geben Sie Ihr Geschlecht an:

[Männlich; Weiblich; Nicht-binär; Keine Antwort]

Wie viele Kinder haben Sie?

[0; 1; ...; 10; Mehr als 10]

Wie alt ist Ihr ältestes Kind?

[0–5; 6–11; 12–15; älter als 16]

Wie alt ist Ihr Kind bzw. wie alt sind Ihre Kinder genau?

Kind 1–10 [unter 1; 1; 2; ...; 18; über 18]

C.2 Demografische Daten 2/2

Wie ist Ihr Familienstand?

- Single;
- Verheiratet oder feste Partnerschaft;
- Verwitwet;
- Geschieden oder getrennt

Was ist Ihr höchster Schulabschluss?

- Kein Abschluss;
- Hauptschulabschluss;
- Realschulabschluss;
- Abitur;
- Fachhochschulreife;
- Bachelor;
- Master/Diplom/Staatsexamen;
- Doktor;
- Keine Angabe

Welche der folgenden Antwortoptionen beschreibt am besten die Gegend, in der Sie wohnen?

- Großstadt (ab 100,000 Einwohner);
- Mittelstadt (ab 20,000 Einwohner);
- Kleinstadt (ab 5,000 Einwohner);
- Landgemeinde

Ich habe durch meinen Beruf Vorwissen im Bereich Datenschutz.

[Stimme gar nicht zu; Stimme nicht zu; Neutral; Stimme zu; Stimme sehr zu]

Sprechen Sie zuhause überwiegend Deutsch?

[Ja; Nein; Keine Antwort]

Haben Sie länger als ... Jahre in Deutschland gelebt?

[1; 3; 5; Keine der Antworten trifft zu.]

Aus welchem Land kommen Sie ursprünglich?

[Freitextfeld]

C.3 Allgemeine Angaben Kind

Welches Geschlecht hat das besagte Kind?

- Männlich
- Weiblich
- Nicht-binär
- Keine Antwort

Hat Ihr Kind eine diagnostizierte Behinderung?

- Nein
- Lernbehinderung
- Sinnesbehinderung
- Innere Erkrankung
- Geistige Behinderung
- Körperliche Behinderung
- Psychische Behinderung
- Keine Antwort
- Sonstiges:

Bitte kreuzen Sie zutreffendes an:

[Nie; Selten; Manchmal; Oft; Immer]

- Mein Kind darf soziale Medien nutzen.
- Mein Kind darf einen Messenger-Dienst (z.B. Whatsapp) benutzen.
- Mein Kind darf online Spiele spielen.

Bitte kreuzen Sie zutreffendes an:

[Ja; Nein]

- Mein Kind hat einen eigenen Social Media Account.
- Mein Kind hat ein Fitnessarmband/eine Smart Watch.
- Mein Kind hat ein eigenes Handy.

C.4 *Parental Privacy Knowledge* [66]

Datenschutzbezogene Faktoren

Wie gut schätzen Sie Ihr Wissen über folgende Themen ein?

[sehr schlecht, schlecht, akzeptabel, gut, sehr gut]

- Übermäßiges Teilen von persönlichen Informationen
- Identitätsdiebstahl und -betrug
- Profiling und Tracking
- Sexting (Senden oder Empfangen von sexuellen Inhalten)
- Cyber-Grooming (sexuelle Ansprache online durch Fremde)
- Kontaktaufnahme durch Fremde
- Missbräuchliche Verwendung von Daten
- Digitale Überwachung
- Cybermobbing

C.5 *Parental Privacy Concern* [66]

Denken Sie bei der Beantwortung der folgenden Fragen bitte weiterhin immer an ihr ältestes Kind.

Ich bin besorgt...

[Überhaupt nicht besorgt; Nicht besorgt; Neutral; Besorgt; Sehr besorgt]

- ...um die digitale Privatsphäre meines Kindes.
- ...darüber, dass mein Kind übermäßig persönliche Informationen über sich teilt.
- ...darüber, dass die Identität meines Kindes online geklaut wird und damit kriminelle Handlungen ausgeführt werden.
- ...darüber, dass mein Kind online getrackt wird und ein Profil über mein Kind angelegt wird.
- ...darüber, dass mein Kind Sexting (Austausch erotischer Texte, Fotos, Videos) betreibt.
- ...darüber, dass mein Kind online sexuell angesprochen wird.
- ...darüber, dass Fremde mein Kind online kontaktieren.
- ...dass Informationen über mein Kindes im Internet missbräuchlich verwendet werden.
- ...dass mein Kind digital überwacht wird.
- ...dass mein Kind Opfer von Cybermobbing wird.

C.6 Child Privacy Victimisation Experience [79]

Welche der folgenden Aktivitäten hat Ihr Kind ausgeführt?

[Nie; Einmal; Mehrmals; Oft; Weiß ich nicht]

- Mein Kind hat Dinge online gepostet/geteilt, die es später bereut hat.
- Mein Kind hat Dinge online gepostet/geteilt, die ich für unangemessen halte.
- Mein Kind hat Sexting betrieben. (Senden oder Empfangen von sexuellen Inhalten)
- Mein Kind hat sich mit jemandem physisch getroffen, den es online kennengelernt hat.

Welche der folgenden Erfahrungen hat Ihr Kind gemacht?

[Nie; Einmal; Mehrmals; Oft; Weiß ich nicht]

- Mein Kind wurde online von Fremden kontaktiert.
- Mein Kind wurde aufgefordert, persönliche Informationen (z.B. Bilder) zu schicken, die es nicht preisgeben wollte.
- Persönliche Informationen (z.B. Bilder) meines Kindes wurden gegen den Willen meines Kindes weitergegeben (z.B. im Klassenchat).

C.7 *Perceived Vulnerability* [5]

Wie wahrscheinlich ist es, ...

[Sehr unwahrscheinlich; unwahrscheinlich; Neutral; Wahrscheinlich; Sehr wahrscheinlich]

- ...dass ihr Kind Opfer einer missbräuchlichen Verwendung von persönlichen Daten wird?
- ...dass andere Kinder Opfer einer missbräuchlichen Verwendung von persönlichen Daten werden?

Wie sehr stimmen Sie den folgenden Aussagen zu?

[Stimme gar nicht zu; Stimme nicht zu; Neutral; Stimme zu; Stimme sehr zu]

- Den Schutz für die digitale Privatsphäre meines Kindes immer aufrecht zu erhalten finde ich anstrengend.
- Niemand in meinem Umfeld benutzt privatsphäre-freundliche alternative Dienste (z.B. Signal, Threema).
- Die gängigen Online-Dienste (z.B. Whatsapp, Zoom) bieten mir mehr Vorteile als privatsphäre-freundliche Alternativen (z.B. mehr Funktionen, bessere Nutzeroberfläche).

C.8 *Parental Online Engagement* [4]

Beantworten Sie die folgenden Fragen.

[Weniger als 1 Stunde am Tag; 1-2 Stunden am Tag; 3-5 Stunden am Tag; 5-9 Stunden am Tag; Mehr als 9 Stunden]

- Wie viel Zeit verbringen Sie täglich im Internet?
- Wie viel Zeit verbringen Sie täglich auf sozialen Medien?
- Wie häufig posten Sie Fotos online?

Beantworten Sie die folgenden Fragen.

[Nie; Seltener; Einmal in der Woche; Einmal am Tag; Mehrfach am Tag]

- Wie oft liken oder kommentieren Sie Beiträge?
- Wie häufig posten Sie Fotos online?

C.9 *Parental Privacy Self-Efficacy* [35, 81, 83, 84]

Wie sehr stimmen Sie den folgenden Aussagen zu?

[Stimme gar nicht zu; Stimme nicht zu; Neutral; Stimme zu; Stimme sehr zu]

- Ich bin zuversichtlich, dass ich die persönlichen Daten meines Kindes online schützen kann.
- Ich bin zuversichtlich, dass ich mich mit den sich verändernden Online-Aktivitäten meines Kindes und den daraus resultierenden Gefahren auf dem Laufenden halten kann.
- Ich weiß, was ich tun muss, wenn die digitale Privatsphäre meines Kindes bedroht ist.
- Ich weiß, an wen ich mich wenden kann, wenn die digitale Privatsphäre meines Kindes bedroht ist.

C.10 *Technical Privacy Skills* [44]

Ich weiß, wie man die folgenden Maßnahmen durchführt:

[Stimme gar nicht zu; Stimme nicht zu; Neutral; Stimme zu; Stimme sehr zu]

- Einstellungen auf dem Handy anpassen, sodass sie meinen Vorstellungen von Privatsphäre-Schutz entsprechen.
- Handy-Einstellungen anpassen, um Einkäufe und Downloads auf dem Handy (duch mein Kind) zu verhindern.

- Handy-Einstellungen anpassen, um Zeitbegrenzungen für Apps einzurichten.
- Auf dem Handy Inhaltsfilter installieren, die nicht altersgerechte Inhalte wegfiltern.
- App-Berechtigungen anpassen, sodass sie meinen Vorstellungen von Privatsphäre-Schutz entsprechen.
- Einstellungen auf Social-Media anpassen, sodass sie meinen Vorstellungen von Privatsphäre-Schutz entsprechen.
- Ein Browser-Plugin installieren, welches Werbe- und Tracking-Cookies blockiert.

C.11 Elternbezogene Faktoren

Wie sehr treffen die folgenden Aussagen zu?

[Stimme gar nicht zu; Stimme nicht zu; Neutral; Stimme zu; Stimme sehr zu]

- Mein Kind wird leicht wütend auf mich.
- Mein Kind bleibt wütend und wehrt sich, nachdem es diszipliniert wurde.
- Der Umgang mit meinem Kind raubt mir Energie.
- Wenn mein Kind schlechte Laune hat, weiß ich, dass uns ein langer und schwieriger Tag bevorsteht.

Wie sehr treffen die folgenden Aussagen zu?

[Stimme gar nicht zu; Stimme nicht zu; Neutral; Stimme zu; Stimme sehr zu]

- Mein Kind scheint verletzt oder verlegen zu sein, wenn ich es korrigiere.
- Mein Kind reagiert stark auf die Trennung von mir.
- Mein Kind ist übermäßig abhängig von mir.
- Ich denke oft an mein Kind, wenn ich bei der Arbeit bin.

Wie sehr treffen die folgenden Aussagen zu?

[Stimme gar nicht zu; Stimme nicht zu; Neutral; Stimme zu; Stimme sehr zu]

- Mein Kind scheint verletzt oder verlegen zu sein, wenn ich es korrigiere.
- Mein Kind reagiert stark auf die Trennung von mir.
- Mein Kind ist übermäßig abhängig von mir.
- Ich denke oft an mein Kind, wenn ich bei der Arbeit bin.

C.12 *Perceived Parental Overload* [44]

Inwieweit stimmen Sie den folgenden Aussagen über Ihre Rolle als Eltern zu?

[Stimme gar nicht zu; Stimme nicht zu; Neutral; Stimme zu; Stimme sehr zu]

- Ich fühle mich von den Anforderungen und der Verantwortung, die ich als Elternteil zu tragen habe, überfordert.
- Es fällt mir schwer, mit den vielfältigen Aufgaben und Verpflichtungen als Elternteil zu jonglieren.
- Als Elternteil habe ich zu wenig Zeit für mich selbst.
- Als Elternteil habe ich viele Sorgen und Themen (z. B. Schulnoten, gesunde Ernährung usw.), um die ich mich kümmern muss.
- Ich nutze Medien, um mein Kind zu unterhalten und einen Moment der Ruhe zu finden.

C.13 *Parental Susceptibility to Peer Influence* [10]

Wie sehr stimmen Sie den folgenden Aussagen hinsichtlich anderer Eltern zu?

[Stimme gar nicht zu; Stimme nicht zu; Neutral; Stimme zu; Stimme sehr zu]

- Ich wende mich oft an andere Eltern, um den besten Weg im Umgang mit den Problemen meines Kindes zu finden.
- Um sicherzugehen, dass ich mich richtig verhalte, beobachte ich oft, wie andere Eltern mit Problemen umgehen.
- Wenn ich Erziehungsentscheidungen treffe, entscheide ich in der Regel so, wie ich denke, dass andere Eltern es gut finden.
- Es ist mir wichtig, an anderen Eltern angebunden zu sein.
- Es ist mir wichtig, Teil von Elterngruppen/-cliquen zu sein.

C.14 *Parental Child Data Disclosure* [4, 81]

Um zu bestätigen, dass Sie die Umfrage aufmerksam lesen, wählen Sie bitte für die folgende Aussage "Neutral" aus.

[Stimme gar nicht zu; Stimme nicht zu; Neutral; Stimme zu; Stimme sehr zu]

Beantworten Sie die folgenden Fragen.

[Nie; Seltener; Einmal in der Woche; Einmal am Tag; Mehrfach am Tag]

- Wie häufig teilen/posten Sie Fotos von Ihrem Kind auf sozialen Medien?
- Wie häufig teilen/posten Sie Fotos von Ihrem Kind in Ihrem Messenger (z.B. Whatsapp) Status?
- Wie häufig teilen/posten Sie Fotos von Ihrem Kind in Ihrem Messenger (z.B. Whatsapp) Profilbild?
- Wie häufig teilen Sie Fotos von Ihrem Kind in privaten Nachrichten?

Mit wem teilen Sie Fotos von Ihrem Kind auf Sozialen Medien

[Eingeschränkter Kreis; Kontakte; Öffentlich; Niemand]

Mit wem teilen Sie Fotos von Ihrem Kind auf Sozialen Medien

[Eingeschränkter Kreis; Kontakte; Öffentlich; Niemand; Weiß nicht]

- Wer kann Ihren Messenger (z.B. Whatsapp) Status sehen?
- Wer kann Ihr Messenger (z.B. Whatsapp) Profilbild sehen?

C.15 *Parental Regulation of Others* [44]

Bitte beantworten Sie die folgenden Fragen. *

[Nie; Selten; Gelegentlich; Häufig; Immer]

- Wenn jemand, den ich nicht kenne, ein Foto von meinem Kind machen möchte, bitte ich ihn, dies nicht zu tun.

- Wenn meine Eltern (Schwiegereltern) ein Foto von meinem Kind teilen möchte, bitte ich sie, dies nicht zu tun.
- Wenn Freunde ein Foto von meinem Kind machen wollen, bitte ich sie, dies nicht zu tun.
- Wenn Freunde ein Foto meines Kindes teilen möchte, bitte ich sie, dies nicht zu tun.

Bitte beantworten Sie die folgenden Fragen. Diese beziehen sich auf das Posten auf Sozialen Medien. Unter "Posten" verstehen wir hier das Posten von Bildern im Profilbild und in Postings.

[Nie; Selten; Gelegentlich; Häufig; Immer]

- Wie oft werden Fotos Ihres Kindes von anderen Personen auf sozialen Medien (erneut) gepostet?
- Wie oft posten Personen, die Sie kennen, Fotos von Ihrem Kind auf sozialen Medien?
- In welchem Ausmaß ermutigen andere Sie, Fotos Ihres Kindes auf sozialen Medien zu posten?
- Wie oft erheben Sie Einwände dagegen, dass andere Fotos von Ihrem Kind auf sozialen Medien posten?

Bitte beantworten Sie die folgenden Fragen. Diese beziehen sich auf das Teilen/Posten in Messengern (z.B. Whatsapp). Unter "Teilen" verstehen wir hier sowohl das Teilen von Bildern in privaten Chats/Gruppenchats sowie das Posten von Bildern in Status und Profilbild.

[Nie; Selten; Gelegentlich; Häufig; Immer]

- Wie oft werden Fotos Ihres Kindes von anderen Personen auf Messengern geteilt?
- Wie oft teilen Personen, die Sie kennen, Fotos von Ihrem Kind auf Messengern?
- In welchem Ausmaß ermutigen andere Sie, Fotos Ihres Kindes auf Messengern zu teilen?
- Wie oft erheben Sie Einwände dagegen, dass andere Fotos von Ihrem Kind auf Messengern teilen?

C.16 *Parental Privacy Mediation Child* [49, 79]

Wie oft treffen Sie die folgenden Maßnahmen, wenn Ihr Kind online ist?

[Nie; Selten; Gelegentlich; Häufig; Immer]

- Ich lese vor der Nutzung einer Website oder App durch mein Kind die Datenschutzrichtlinien.
- Ich verwende Kindersicherungen, um die Online-Aktivitäten meines Kindes zu blockieren, zu filtern oder zu überwachen.
- Ich helfe meinem Kind beim Einrichten der Datenschutzeinstellungen.
- Ich suche online nach den Daten meines Kindes.
- Ich spreche mit meinem Kind über meine Bedenken bezüglich seiner Online-Postings.
- Ich kommentiere oder antworte direkt auf die Online-Postings meines Kindes.
- Ich sitze bei meinem Kind, wenn es persönliche Daten angibt.
- Ich sitze bei meinem Kind, wenn es Online-Formulare/Quizfragen ausfüllt.
- Ich kontrolliere die persönlichen Nachrichten meines Kindes.
- Ich nutze für mein Kind Technologien zur Verbesserung des Datenschutzes (PETs).
- Ich lösche die Cookies nach den Online-Sitzungen meines Kindes.
- Ich schränke ein/verbiete meinem Kind die Nutzung von Webseiten und Apps, die persönliche Daten abfragen.

Wie oft treffen Sie die folgenden Maßnahmen, wenn Sie selber online sind?

[Nie; Selten; Gelegentlich; Häufig; Immer]

- Ich gebe online den richtigen Namen meines Kindes an.
- Ich gebe online das Geburtsdatum meines Kindes an.
- Ich verwende online einen falschen Namen oder einen falschen Ausweis für mein Kind.
- Ich gebe online unvollständige Informationen über mein Kind an.
- Ich greife auf andere Websites/Apps zurück, die nicht nach den persönlichen Daten meines Kindes fragen.

Bitte beantworten Sie die folgenden Fragen.

[uneingeschränkt; nicht in peinlichen Situationen; nur voll angezogen; nur von hinten; nur mit verschwommenem Gesicht; nur mit einem Smiley über dem Gesicht; gar nicht]

- Wie zeigen Sie Ihr Kind auf Fotos, die Sie in sozialen Medien posten (Posting oder Profilbild)?
- Wie zeigen Sie Ihr Kind auf Fotos, die Sie in Ihrem Messenger (z.B. WhatsApp) teilen?
- Wie zeigen Sie Ihr Kind auf Fotos, die Sie in Ihrem Messenger (z.B. Whatsapp) Profilbild teilen?
- Wie zeigen Sie Ihr Kind auf Fotos, die Sie in privaten Nachrichten teilen?

D Survey (Translated into English)

D.1 Demographic Data 1/2

How old are you?

[under 18; 18; 19; ...; 75; older than 75]

Please indicate your gender:

[Male; Female; Non-binary; No answer]

How many children do you have?

[0; 1; ...; 10; More than 10]

How old is your oldest child?

[0–5; 6–11; 12–15; older than 16]

How old is your child / how old are your children exactly?

Child 1–10 [under 1; 1; 2; ...; 18; over 18]

D.2 Demographic Data 2/2

What is your marital status?

- Single
- Married or in a committed partnership
- Widowed
- Divorced or separated

What is your highest educational degree?

- No degree
- Lower secondary school certificate
- Intermediate secondary school certificate
- High school diploma (Abitur)
- University of applied sciences entrance qualification
- Bachelor
- Master/Diploma/State examination
- Doctorate
- No answer

Which of the following best describes the area in which you live?

- Large city (from 100,000 inhabitants)
- Medium-sized city (from 20,000 inhabitants)
- Small town (from 5,000 inhabitants)
- Rural municipality

Through my profession, I have prior knowledge in the field of data protection.

[Strongly disagree; Disagree; Neutral; Agree; Strongly agree]

Do you predominantly speak German at home?

[Yes; No; No answer]

Have you lived in Germany for more than ... years?

[1; 3; 5; None of the answers apply]

Which country are you originally from?

[Free text]

D.3 General Information About the Child

What is the gender of the child in question?

- Male
- Female
- Non-binary
- No answer

Does your child have a diagnosed disability?

- No
- Learning disability
- Sensory disability
- Internal/medical condition
- Intellectual disability
- Physical disability
- Psychological disability
- No answer
- Other:

Please select what applies:

[Never; Rarely; Sometimes; Often; Always]

- My child is allowed to use social media.
- My child is allowed to use a messenger service (e.g., WhatsApp).
- My child is allowed to play online games.

Please select what applies:

[Yes; No]

- My child has their own social media account.
- My child has a fitness tracker / smartwatch.
- My child has their own mobile phone.

D.4 *Parental Privacy Knowledge* [66]

How well do you assess your knowledge on the following topics?

[very poor; poor; acceptable; good; very good]

- Oversharing of personal information
- Identity theft and fraud
- Profiling and tracking
- Sexting (sending or receiving sexual content)
- Cyber-grooming (sexual approaches online by strangers)
- Contact by strangers
- Misuse of data
- Digital surveillance
- Cyberbullying

D.5 *Parental Privacy Concern* [66]

When answering the following questions, please continue to think of your oldest child.

I am concerned…

[Not concerned at all; Not concerned; Neutral; Concerned; Very concerned]

- …about my child's digital privacy.
- …that my child shares too much personal information.
- …that my child's identity is stolen online and used for criminal activities.
- …that my child is tracked online and a profile is created about them.
- …that my child engages in sexting (exchange of erotic texts, photos, videos).
- …that my child is approached sexually online.
- …that strangers contact my child online.
- …that information about my child is misused on the internet.
- …that my child is digitally monitored.
- …that my child becomes a victim of cyberbullying.

D.6 *Child Privacy Victimization Experience* [79]

Which of the following activities has your child engaged in?

[Never; Once; Several times; Often; I don't know]

- My child has posted/shared things online that they later regretted.
- My child has posted/shared things online that I consider inappropriate.
- My child has engaged in sexting (sending or receiving sexual content).
- My child has met someone in person whom they first met online.

Which of the following experiences has your child had?

[Never; Once; Several times; Often; I don't know]

- My child has been contacted online by strangers.
- My child has been asked to send personal information (e.g., photos) that they did not want to share.
- Personal information (e.g., photos) of my child has been shared without their consent (e.g., in a class group chat).

D.7 *Perceived Vulnerability* [5]

How likely is it that ...

[Very unlikely; Unlikely; Neutral; Likely; Very likely]

- ... your child will fall victim to improper use of personal information?
- ... other children will fall victim to improper use of personal information?

To what extent do you agree with the following statements?

[Strongly disagree; Disagree; Neutral; Agree; Strongly agree]

- I find it exhausting to constantly maintain the protection of my child's digital privacy.
- No one in my social environment uses privacy-friendly alternative services (e.g., Signal, Threema).
- Mainstream online services (e.g., WhatsApp, Zoom) offer me more advantages than privacy-friendly alternatives (e.g., more features, better usability).

D.8 *Parental Online Engagement* [4]

Please answer the following questions.

[Less than 1 hour per day; 1–2 hours per day; 3–5 hours per day; 5–9 hours per day; More than 9 hours]

- How much time do you spend online each day?
- How much time do you spend on social media each day?
- How often do you post photos online?

Please answer the following questions.

[Never; Rarely; Once a week; Once a day; Several times a day]

- How often do you like or comment on posts?
- How often do you post photos online?

D.9 *Parental Privacy Self-Efficacy* [35, 81, 83, 84]

To what extent do you agree with the following statements?

[Strongly disagree; Disagree; Neutral; Agree; Strongly agree]

- I am confident that I can protect my child's personal data online.
- I am confident that I can keep up with my child's evolving online activities and the risks that arise from them.
- I know what to do when my child's digital privacy is threatened.
- I know whom to contact when my child's digital privacy is threatened.

D.10 *Technical Privacy Skills* [44]

I know how to perform the following actions:

[Strongly disagree; Disagree; Neutral; Agree; Strongly agree]

- Adjust smartphone settings so that they align with my privacy preferences.
- Adjust smartphone settings to prevent purchases and downloads (by my child).
- Adjust smartphone settings to set time limits for apps.
- Install content filters on the smartphone that block age-inappropriate content.
- Adjust app permissions so that they align with my privacy preferences.
- Adjust privacy settings on social media platforms to match my privacy preferences.
- Install a browser plugin that blocks advertising and tracking cookies.

D.11 *Parenting-Related Factors*

How much do the following statements apply to your child?

[Strongly disagree; Disagree; Neutral; Agree; Strongly agree]

- My child gets angry with me easily.
- My child stays angry and resists after being disciplined.
- Managing my child drains my energy.
- When my child is in a bad mood, I know a long and difficult day lies ahead.

How much do the following statements apply to your child?

[Strongly disagree; Disagree; Neutral; Agree; Strongly agree]

- My child seems hurt or embarrassed when I correct them.
- My child reacts strongly to being separated from me.
- My child is overly dependent on me.
- I often think about my child while I am at work.

D.12 *Perceived Parental Overload* [44]

To what extent do you agree with the following statements about your role as a parent?

[Strongly disagree; Disagree; Neutral; Agree; Strongly agree]

- I feel overwhelmed by the demands and responsibilities I carry as a parent.
- I find it difficult to juggle the various tasks and obligations associated with being a parent.
- As a parent, I have too little time for myself.
- As a parent, I have many concerns and issues to deal with (e.g., school grades, healthy nutrition).
- I use media to keep my child entertained so I can have a moment of rest.

D.13 *Parental Susceptibility to Peer Influence* [10]

To what extent do you agree with the following statements about other parents?

[Strongly disagree; Disagree; Neutral; Agree; Strongly agree]

- I often turn to other parents to find the best way to handle my child's problems.
- To make sure I am doing the right thing, I often observe how other parents deal with problems.
- When making parenting decisions, I usually choose what I think other parents would approve of.
- It is important to me to stay connected with other parents.
- It is important to me to be part of parent groups or parent circles.

D.14 *Parental Child Data Disclosure* [4, 81]

To confirm that you are reading the survey carefully, please select "Neutral" for the following statement.

[Strongly disagree; Disagree; Neutral; Agree; Strongly agree]

Please answer the following questions.

[Never; Rarely; Once a week; Once a day; Multiple times a day]

- How often do you share/post photos of your child on social media?
- How often do you share/post photos of your child in your messenger status (e.g., WhatsApp)?
- How often do you share/post photos of your child as your messenger profile picture (e.g., WhatsApp)?
- How often do you share photos of your child in private messages?

With whom do you share photos of your child on social media?

[Restricted group; Contacts; Public; Nobody]

Who can view your child's photos in messenger apps?

[Restricted group; Contacts; Public; Nobody; Don't know]

- Who can see your messenger status (e.g., WhatsApp)?
- Who can see your messenger profile picture (e.g., WhatsApp)?

D.15 *Parental Regulation of Others* [44]

Please answer the following questions.

[Never; Rarely; Occasionally; Frequently; Always]

- If someone I don't know wants to take a photo of my child, I ask them not to do so.
- If my parents (or in-laws) want to share a photo of my child, I ask them not to do so.
- If friends want to take a photo of my child, I ask them not to do so.
- If friends want to share a photo of my child, I ask them not to do so.

Please answer the following questions. These refer to posting on social media. By "posting," we mean uploading photos as a profile picture or in posts.

[Never; Rarely; Occasionally; Frequently; Always]

- How often are photos of your child (re)posted on social media by others?
- How often do people you know post photos of your child on social media?
- To what extent do others encourage you to post photos of your child on social media?
- How often do you object when others post photos of your child on social media?

Please answer the following questions. These refer to sharing/posting in messengers (e.g., WhatsApp). By "sharing," we mean sending images in private or group chats, as well as posting them in status or profile photos.

[Never; Rarely; Occasionally; Frequently; Always]

- How often are photos of your child shared on messengers by others?
- How often do people you know share photos of your child on messengers?
- To what extent do others encourage you to share photos of your child on messengers?
- How often do you object when others share photos of your child on messengers?

D.16 *Parental Privacy Mediation Child* [49, 79]

How often do you take the following actions when your child is online?

[Never; Rarely; Sometimes; Often; Always]

- I read the privacy policies of a website or app before my child uses it.
- I use parental controls to block, filter, or monitor my child's online activities.
- I help my child configure privacy settings.
- I search online for information about my child.
- I talk with my child about my concerns regarding their online postings.
- I comment on or directly respond to my child's online posts.
- I sit next to my child when they enter personal information online.
- I sit next to my child when they fill in online forms or quizzes.
- I check my child's private messages.
- I use privacy-enhancing technologies (PETs) for my child.
- I delete cookies after my child's online sessions.
- I restrict or prohibit my child from using websites or apps that request personal data.

How often do you take the following actions when *you* are online?

[Never; Rarely; Sometimes; Often; Always]

- I provide my child's real name online.
- I provide my child's date of birth online.
- I use a false name or false identity for my child online.
- I provide incomplete information about my child online.
- I use websites/apps that do not ask for personal data about my child.

Please answer the following questions.

[Unrestricted; Not in embarrassing situations; Only fully clothed; Only from behind; Only with blurred face; Only with an emoji covering the face; Not at all]

- How do you show your child in photos you post on social media (posts or profile pictures)?
- How do you show your child in photos you share via messenger apps (e.g., WhatsApp)?
- How do you show your child in photos you use as your messenger (e.g., WhatsApp) profile picture?
- How do you show your child in photos you share in private messages?