

USENIX

THE ADVANCED COMPUTING
SYSTEMS ASSOCIATION

SoK: The Design Space of Usable Privacy Interventions for Parents: A Systematization of Knowledge

Ann-Kristin Lieberknecht, *Goethe University Frankfurt;*
Sascha Loebner, *University of Hamburg*

https://www.usenix.org/conference/soups2026/presentation/lieberknecht

This paper is included in the Proceedings of the
Twenty-Second Symposium on Usable Privacy and Security.

August 24–26, 2026 • Hannover, Germany

ISBN 978-1-939133-59-5

Open access to the Proceedings of the
Twenty-Second Symposium on Usable Privacy and Security
is sponsored by USENIX.

SoK: The Design Space of Usable Privacy Interventions for Parents: A Systematization of Knowledge

Ann-Kristin Lieberknecht
Goethe University Frankfurt

Sascha Löbner
University of Hamburg

Abstract

Privacy and security risks increasingly emerge through everyday family technology use, requiring families to navigate complex decisions about children's data and digital participation. Parents play a central role in these processes, interpreting risks, configuring technologies, and negotiating privacy practices with children while adapting to rapidly evolving digital environments. Research addressing these challenges spans multiple communities, including usable privacy, family human–computer interaction, and digital literacy, yet remains fragmented across studies of parental experiences, behavioral determinants, and intervention design. This paper presents a systematization of knowledge synthesizing how research has approached supporting parental privacy practices. We compile a focused corpus combining evaluated interventions, parent-focused empirical pre-studies, and quantitative investigations of behavioral determinants. We develop an analytic framework distinguishing intended parental learning outcomes from the design features through which support is operationalized, enabling comparison across heterogeneous evidence. Mapping interventions against this framework and relating them to empirical patterns reveals how knowledge about parents' privacy challenges is selectively translated into implemented forms of support. The results highlight recurring concentrations and gaps in parental privacy interventions and illuminate the practical challenges of enabling privacy practices within everyday family life.

Copyright is held by the author/owner. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee.
USENIX Symposium on Usable Privacy and Security (SOUPS) 2026.
August 23–26, 2026, Hannover, Germany.

1 Introduction

Children's digital privacy has become a critical societal concern as data about children is increasingly generated, collected, and shared through everyday family interactions with digital technologies [7,37]. Regulatory enforcement under the GDPR and empirical audits alike reveal persistent deficiencies in protecting children's personal data, including unlawful processing by major platforms [8, 13, 14] and widespread practices such as undisclosed data collection, third-party sharing, and inadequate privacy protections in children's apps [17, 47, 49]. This evidence suggests that risks to children's privacy are embedded in the digital ecosystems families rely on rather than arising from isolated failures [7].

Within these ecosystems, parents act as primary proxy decision makers for their children across diverse contexts [22, 25, 27, 44]. These decisions shape children's data traces and influence exposure to profiling and long-term privacy risks [7], yet parents must navigate opaque data flows, asymmetric power relations, and institutional requirements with limited insight into how children's data are actually collected, processed, or shared [15, 17, 27, 47, 49, 60]. As a result, even motivated parents may struggle to make informed or consistent privacy decisions [60].

Supporting parents under these conditions has emerged as an important goal for privacy research and design [22, 25, 27, 29, 44]. Yet although parents' central role is widely recognized and concerns about children's privacy are consistently reported [9, 15, 32, 61], only a small number of interventions have been explicitly designed and evaluated with parents as the primary target group [27, 29]. Relevant research is further fragmented across partially disconnected strands, including empirically evaluated privacy interventions, quantitative studies examining determinants of parental privacy behavior, qualitative and mixed-methods work eliciting parents' needs and concerns, and design guideline papers addressing children's privacy more broadly [15, 59, 60]. This fragmentation makes it difficult to compare approaches, synthesize heterogeneous findings, or translate empirical insights into concrete design

decisions for those seeking to support parents. Systematization is therefore needed not only to organize existing work but also to surface the gaps and absences shaping the parental privacy intervention design space.

This paper presents a Systematization of Knowledge (SoK) on designing privacy interventions for parents. Our goal is to organize and synthesize design-relevant knowledge on how privacy interventions can support parents in making privacy decisions for their children under real-world constraints. This encompasses identified parental support needs, proposed design features, mechanisms for parental assistance, and empirically evaluated interventions. Beyond organizing existing work, the synthesis aims to explain how empirical knowledge about parental privacy practices is translated into implemented forms of support, thereby revealing structural patterns shaping the emerging intervention design space.

This SoK makes the following contributions.

- A systematic identification and synthesis of the empirical evidence base related to parental privacy interventions and parental privacy behavior.
- A design criteria framework distinguishing intended learning outcomes from design features of parental privacy support, enabling systematic comparison of how interventions are conceptualized and operationalized across studies.
- A mapping and gap analysis of existing interventions that identifies recurring concentrations, conceptual–operational gaps, and underrepresented areas within the current intervention landscape.
- An analysis of structural tensions shaping the intervention design space, including trade-offs between simplification for accessibility and the development of reflective judgment, between parental responsibility and distributed family expertise, and between depth of support and scalability.

2 Background and Related Work

2.1 Parental Privacy and Security as a Design Context

Prior work in usable privacy and security has already developed design frameworks and educational models aimed at fostering children's privacy literacy and digital autonomy. These approaches conceptualize privacy learning as the development of individuals' ability to interpret data practices, understand information flows, evaluate risks, and make informed decisions in digital environments (e.g., [26, 52]). Reviews of cybersecurity education tools similarly emphasize instructional strategies designed to increase awareness, knowledge, and decision-making competence among end users through structured learning activities and interactive educational formats [59]. These frameworks provide important conceptual and pedagogical foundations that are also relevant to parents, who must develop comparable understandings in order to guide children's digital participation and support privacy learning within everyday family life.

However, parents represent a distinct design context for privacy and cybersecurity interventions. Unlike individuals managing only their own personal information, parents act as proxy decision-makers for children [22, 25, 27, 44] while also shaping children's data traces through their own disclosures [5, 25, 48]. Communication Privacy Management theory conceptualizes these situations as involving shared ownership of information and negotiated privacy boundaries within relationships [43]. Parental privacy decisions are embedded in networks of stakeholders, co-parents, extended family members, educators, and online platforms, each bringing different expectations and norms regarding information sharing [25]. Further, they are shaped by competing concerns: the imperative to support children's participation and autonomy, and the desire to protect children from harm [5, 7, 25, 27]. Parents may simultaneously fear the consequences of underprotection and over-control, navigate disagreements with children or co-parents, and operate with incomplete understanding of the technological systems mediating their children's lives [15, 17, 27, 60]. However, these tensions are not resolved once but revisited repeatedly as children develop and digital environments change [27]. As a consequence, effective privacy support for parents requires approaches that go beyond one-time risk communication or isolated skill-building. Instead, it must account for the recurring, emotionally charged, and relationally embedded conditions under which privacy and security decisions are made in everyday family life, spanning both the supervision of children's activity and the shared management of family information.

2.2 Empirical Work on Supporting Parents' Privacy and Security Decisions

Research addressing parental privacy and cybersecurity support spans multiple empirical traditions. Only a small number of studies introduce and evaluate interventions explicitly designed to support parents or families in privacy and cybersecurity contexts, employing diverse educational, interactive, and collaborative formats, including [2, 3, 11, 18, 46, 50]. A larger body of work examines how parents understand and manage privacy and cybersecurity challenges in everyday family contexts, primarily through qualitative interviews and family studies. They document a range of strategies parents employ to navigate these challenges, including active discussion, monitoring, restrictions, and technical controls [33, 34, 40, 56], with research highlighting developmental trade-offs: restrictive approaches may reduce short-term exposure to risks, while conversational and instructive approaches support children's

development of privacy awareness and coping skills [10, 33]. Studies also document challenges such as declining adolescent engagement and difficulties discussing abstract privacy concepts [4, 53]. Other work situates privacy management within broader family dynamics, showing how families employ combinations of technological safeguards, rules, communication, and social support networks when addressing online risks [39]. Parenting style, digital literacy, and household role distribution further influence coping strategies and responsibility allocation [23, 45]. Similarly, studies of parent–child dyads indicate that conversational approaches can support deeper understanding of privacy concepts among children [54]. Quantitative studies further identify parental self-efficacy as a central predictor of mediation behaviors, with technical skills as an important antecedent and confidence declining as children grow older [19, 28].

Together, these strands generate substantial knowledge relevant to designing privacy and cybersecurity support for parents. Yet this knowledge remains fragmented across partially disconnected research traditions, motivating the systematic synthesis presented in this paper.

3 Methodology

3.1 Systematic Literature Identification

To synthesize existing knowledge on interventions supporting parents in privacy- and cybersecurity-related decision-making, we conducted a systematic literature identification and screening process following PRISMA 2020 guidelines [41]. The search targeted four major peer-reviewed digital libraries: ACM Digital Library, IEEE Xplore, SpringerLink, and Elsevier ScienceDirect, which together cover primary publication venues for usable privacy and security research, human–computer interaction, and interdisciplinary work on technology use in families and educational contexts. The search was limited to English-language peer-reviewed publications published from 2015 onward to reflect contemporary digital platforms and privacy challenges.

The search string combined three conceptual components: (1) intervention and learning support, (2) privacy and cybersecurity context, and (3) parent and family relevance. Search terms were applied to titles and abstracts as follows:

> Title:(("training" OR "education" OR "literacy" OR "intervention" OR "learning" OR "curriculum" OR "course" OR "support*") AND ("privacy" OR "secur*" OR "cybersecurity" OR "data protection" OR "online safety" OR "digital safety" OR "media" OR "internet" OR "social media")) AND Abstract:("parent*" OR "family" OR "caregiver*")

The search yielded 517 records. Screening was conducted in three stages: (1) title screening to remove clearly irrelevant work, (2) abstract screening when relevance could not be determined by title alone, and (3) full-text screening when eligibility remained unclear. Two independent screening stages were conducted, and borderline cases were conservatively deferred to full-text review. Cohen's Kappa for the screening process was 0.80. Screening followed predefined inclusion criteria:

1. **Target population:** Studies explicitly focused on parents or caregivers. Child-focused studies were included only when parents actively participated beyond logistical support. During full-text screening, 7 child-only studies were excluded because they did not involve active parental participation, although some were retained as contextual background references.

2. **Intervention relevance:** Studies proposing, implementing, evaluating, or empirically informing approaches intended to support parents in managing children's privacy and cybersecurity were included. This encompassed studies generating design-relevant knowledge, such as identified parental support needs, proposed design features, mechanisms for parental assistance, or evaluated forms of support. Purely descriptive studies reporting awareness, concerns, or attitudes without deriving actionable implications for parental support or intervention design were excluded.

3. **Publication quality:** Only peer-reviewed papers were included. No exclusions were made based on publication labels (e.g., full papers, short papers, workshop papers). However, the final corpus consisted exclusively of full papers. Papers lacking sufficient methodological detail were excluded during full-text screening

Duplicate and overlapping studies were manually identified through comparisons of titles, authors, study descriptions, and reported methods. In cases of overlapping publications, the most complete version was retained unless multiple papers contributed distinct empirical findings.

After screening, 119 papers remained for full-text analysis, of which 22 papers were included in the final corpus. Backward and forward citation searches were conducted on 11 papers [4, 6, 11, 21, 24, 29, 31, 51, 57, 58, 62] to mitigate limitations of keyword-based search in this interdisciplinary domain. These papers were selected based on their centrality and relevance to parental privacy and cybersecurity interventions. Additional records from citation searching underwent the same screening procedure and inclusion criteria.

The final corpus consists of seven evaluated plus one proposed parental privacy and security interventions, 13 parent-focused pre-studies eliciting needs and expectations, and one quantitative studies examining determinants of parental behavior. A PRISMA flow diagram summarizes the identification and screening process (cf. Figure 1). Because the reviewed intervention literature remains comparatively small and heterogeneous, the resulting framework and mappings should

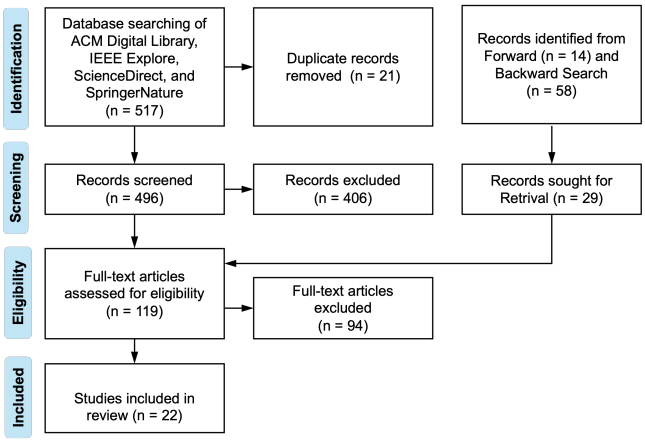


Figure 1: Flow diagram of literature screening process following [41].

be interpreted as analytical structures for identifying emerging patterns and design directions rather than as exhaustive categorizations of the field.

3.2 Evidence Synthesis

The unit of analysis was a design-relevant evidence snippet, defined as any passage articulating a design choice, assumption, constraint, or observed outcome related to parental privacy or cybersecurity support that could inform the design or operationalization of interventions.

The framework was developed through an iterative qualitative process. Initial familiarization with the corpus informed the inductive development of a preliminary codebook, which was collaboratively refined by three researchers to improve conceptual clarity and coverage. Pilot coding on a subset of studies supported iterative revision of codes and category definitions through discussion. Final coding was conducted by the primary author and independently reviewed by a second researcher, with discrepancies resolved through consensus. Framework development did not employ formal inter-rater reliability measures, as the process involved iterative and interpretive qualitative coding rather than fixed classification, consistent with established qualitative research practices in CSCW and HCI [38].

The two analytical dimensions, intended learning outcomes and design features of parental privacy support, emerged during the coding process and were found to consistently capture design-relevant aspects across both empirical and intervention studies. Learning outcomes captured capabilities or orientations that support mechanisms aimed to foster (e.g., conceptual understanding or technical skills). Design features captured how support was operationalized, including participation structures, learning arrangements, and engagement strategies. Coding was interpretive and qualitative and was applied consistently across evaluated interventions, parent-focused pre-studies, and complementary empirical work. Tags were intentionally non-exclusive to preserve overlap between concepts during evidence extraction.

Each snippet was additionally coded for whether a design aspect was implemented, conceptually proposed, or explicitly reported as absent. Absence was coded only when explicitly stated by the original authors.

Following extraction, coded elements were iteratively compared across papers to identify recurring dimensions along which existing work varied in conceptualizing or operationalizing parental privacy support. These dimensions were refined into a set of analytic design criteria that organize design-relevant knowledge reflected in the literature rather than prescribing intervention strategies. The resulting criteria form the basis of the framework presented in Section 4 and the subsequent mapping and gap analysis in Section 5.

Existing design guideline papers related to children's and family privacy were examined as a conceptual reference layer but were not included in the coding process, as they do not constitute empirical evidence of parental support needs or intervention designs. They are instead discussed comparatively in Section 6.

4 Design Criteria Framework

4.1 State of Evidence Base

The final corpus comprises three strands of research addressing parental privacy and cybersecurity in family contexts from distinct empirical and design perspectives.

Pre-studies: The largest strand consists of formative empirical research examining how parents navigate digital risks in family contexts. Rather than evaluating interventions, these studies investigate motivators of parental privacy engagement, parent–child communication practices, and constraints related to skills, responsibilities, and social roles. Evidence from this strand makes visible contextual conditions and behavioral mechanisms shaping the design space for parental privacy and cybersecurity support.

Interventions: Intervention studies examine support-oriented approaches intended to strengthen families' engagement with privacy and cybersecurity challenges. These include educational programs, facilitation approaches for parent–child communication, virtual learning environments, collaborative games, and in-home toolkits designed to render data practices visible within everyday family settings. While broader digital or AI literacy initiatives exist, this review focuses on interventions explicitly oriented toward parental privacy and cybersecurity.

Parental Control: Research on parental control technologies addresses similar risk domains but focuses on technological mechanisms structuring parent–child oversight and mediation. This strand provides an important reference point

for prevailing design assumptions surrounding parental involvement in digital safety. Recent work increasingly explores alternatives to unilateral monitoring, describing collaborative or negotiated oversight models emphasizing shared decision-making and joint engagement. Of the 22 papers in the corpus, eight examine parental control technologies through implemented systems or analytical investigations of existing tools and practices.

Taken together, the evidence base suggests three strands of research that appear to have developed unevenly and largely in parallel. Formative studies characterize how parents experience and navigate privacy and cybersecurity challenges, while only a limited number of studies translate these insights into evaluated forms of support. Research on parental control technologies represents a more developed body of work but concentrates on a comparatively narrow design space centered on structuring oversight of children's digital environments. Knowledge about parental privacy and cybersecurity therefore appears distributed across studies addressing related problems from different perspectives without consistently connecting their design assumptions or contributions.

A comprehensive overview of all included studies is provided in the Appendix A.

4.2 Overview of the Framework

This section presents the primary analytic outcome of the evidence synthesis: a design criteria framework organizing design-relevant knowledge from existing research on parental privacy and cybersecurity. The criteria represent analytic constructs capturing recurring considerations, constraints, and dimensions of variation reflected in how prior work conceptualizes and operationalizes parental privacy support. The framework distinguishes two complementary analytical perspectives observed across the literature: 1) intended learning outcomes, describing capabilities families develop or exercise, including conceptual understanding, evaluative reflection, technical enactment, parental self-efficacy, and parent–child communication, and 2) design features, capturing how support is operationalized through participation organization, learning structure, and engagement environments. Certain themes appear across both perspectives, most notably communication, though each addresses a distinct analytical object: communicative practices within families on the one hand, and how interventions configure interaction and participation environments on the other. Distinguishing between these two perspectives allows the framework to reveal how intended learning objectives are reflected in the design choices through which interventions are realized.

Table 1: Overview of design criteria and representative aspects identified across the evidence base. Aspects are illustrative rather than exhaustive.

Design Criterion	Representative Aspects (Examples)
Understanding of Privacy Risks and Data Practices	Risk Awareness; Platform Data Practices; Tracking and Data Collection; System-Level Understanding; Privacy Consequences; Everyday Scenarios
Reflective Evaluation in Digital Privacy Situations	Self-Reflection on Practices; Contextual Risk Evaluation; Everyday Decision-Making; Perspective Comparison; Ecosystem-Level Reflection
Technical Enactment of Privacy Protection	Privacy Setting Configuration; Permission and Access Management; Tool-Based Controls; Guided Walkthroughs; Hands-On Practice
Parental Self-Efficacy in Privacy Management	Confidence Building; Reducing Technological Anxiety; Supported Sense of Agency; Collaborative Competence Building; Adaptive Parental Role Support
Parent–Child Privacy Communication	Open Privacy Dialogue; Joint Privacy Interpretation; Negotiation of Privacy Decisions; Reciprocal Parent–Child Learning; Shared Responsibility Framing
Organization of Privacy Support	Parent-Only Participation; Joint Parent–Child Participation; Facilitated or Institutional Support; Artifact-Guided Interaction; Community or Peer-Based Support
Designing Learning in Privacy Support	Structured Learning Progression; Developmentally Adapted Learning; Guided Practice Activities; Differentiated Learning Paths
Communication and Engagement in Privacy Support	Narrative or Scenario Framing; Relatable Everyday Contexts; Interactive Engagement Formats; Tangible or Visual Representations; Playful or Gamified Engagement; Emotionally Moderated Framing

4.3 Design Criteria Related to Intended Learning Outcomes

Research characterizes parental privacy mediation as a constellation of interrelated yet analytically distinct capability dimensions identified across studies. Although closely connected in practice, these distinctions reflect analytical perspectives emerging from the literature rather than a sequential or hierarchical progression of competencies.

4.3.1 Understanding of Privacy Risks and Data Practices

Understanding of privacy risks and data practices captures how studies describe parents' conceptual understanding of

online privacy and cybersecurity, including awareness of data practices and recognition of threats. A recurring observation concerns parents' limited awareness of personal data generation and platform data processing [29, 50]. Evidence further indicates misaligned threat perceptions, with risks frequently attributed to unknown external actors rather than everyday social interactions [29]. Limited technological understanding is described as constraining parents' ability to interpret privacy settings or recognize available protection strategies [29, 50]. Studies further link these knowledge gaps to family dynamics: as children develop greater platform familiarity, parental proficiency may decline relative to children's expertise. This shift in perceived competence is associated with shifts in authority within family privacy discussions [1, 46]. Evidence indicates that conceptual awareness alone rarely translates directly into effective mediation, instead functioning as an informational foundation requiring contextual interpretation within family decision-making situations [29, 50]. Research therefore characterizes conceptual understanding as foundational yet limited when detached from everyday application contexts.

4.3.2 Evaluative Judgment in Digital Privacy Situations

Evaluative judgment in privacy contexts emerges in the literature as parents' ability to interpret privacy situations, reflect on practices, and form context-sensitive judgments within family life. Research describes evaluative judgment as extending beyond conceptual awareness toward interpretation of implications in everyday contexts. Privacy aware behavior is frequently linked to reflection on personal practices, including decisions about sharing children's information or selecting privacy-respecting services [27]. Reflective awareness is associated with increased engagement in mediation practices [28]. A consistent theme involves evaluation as a situated interpretive process shaped through lived experience rather than abstract knowledge alone. Collaborative interaction frequently provides contexts in which such reasoning emerges despite distributed expertise [54]. Intervention-oriented studies likewise describe reflective activities structured around narratives, scenarios, and shared deliberation under ambiguity [4, 30, 50].

4.3.3 Technical Enactment of Privacy Protection

A recurring theme across studies concerns parents' ability to translate privacy intentions into procedural actions such as configuring settings or managing permissions. Findings indicate that privacy-related mediation places substantial technical demands on parents, with procedural competence showing stronger associations with self-efficacy than abstract knowledge alone [27–29]. Awareness-oriented approaches are frequently described as insufficient when practical configuration knowledge is lacking. Parents are repeatedly described as valuing actionable, application-specific guidance supporting real-world task execution [11, 53]. Research therefore characterizes this capability as grounded in situated procedural competence rather than abstract knowledge alone. Studies report it appearing both indirectly through familiarity-building and directly through interaction with configurable environments [1, 3, 11, 16, 18]. Translating intended protections into sustained practice is described as challenging, positioning procedural engagement with everyday digital environments as an ongoing rather than one-time achievement.

4.3.4 Parental Self-Efficacy in Privacy Management

Self-efficacy in privacy management is positioned in the literature as parents' perceived capability and legitimacy to act in managing privacy challenges. Across studies, parental self-efficacy emerges as a central psychological factor shaping engagement with mediation. Evidence links technological anxiety and perceived lack of competence to reduced engagement, while higher confidence is associated with more diverse mediation practices [27, 29]. Findings further indicate perceived capability may influence behaviour more strongly than concern alone [28]. Research also portrays self-efficacy as relationally shaped within family dynamics. Parents are frequently described as engaging in collaborative learning with children under conditions of distributed expertise [54]. Increasing child autonomy is associated with declining parental confidence linked to reduced visibility into online activity [28]. Design-oriented studies illustrate how interaction structures influence perceived authority and competence depending on how responsibility is distributed within systems [1–3, 16, 20]. Taken together, the literature portrays self-efficacy as a socially negotiated perception of agency emerging within evolving family relationships.

4.3.5 Parent–Child Privacy Communication

Parent–Child privacy communication captures how research portrays families' ability to engage in meaningful dialogue about privacy and cybersecurity. A recurring observation concerns difficulties sustaining concrete privacy discussions, with conversations often remaining abstract and limiting shared understanding [53]. Communication challenges are linked to asymmetries in awareness, parental uncertainty, and adolescents' resistance to authority-driven discussions [1, 4, 11, 27, 53]. At the same time, evidence consistently associates reciprocal communication with positive outcomes. Studies describe shifts from one-directional guidance toward collaborative exchanges in which children contribute knowledge and initiate discussions [4, 30, 50]. Shared experiences and common reference points are described as facilitating dialogue even when parents lack technical expertise [39, 54]. Communication is therefore portrayed as a relational capability enacted through situated interaction practices enabling families to interpret and negotiate privacy decisions.

4.4 Design Criteria Related to Design Features

Across design-feature criteria, variation is described in how participation, learning activities, and engagement environments are organized.

4.4.1 Organization of Privacy Support

Studies suggest privacy support benefits from organizational embedding rather than passive information availability. Evidence indicates parents rarely seek privacy resources proactively, suggesting engagement depends on outreach integrated into familiar environments [29]. Privacy support is therefore frequently situated within institutional contexts such as schools or community services as well as incidental everyday environments [29]. Informal learning spaces may similarly integrate privacy engagement into exploratory family activities [30]. Research further portrays privacy mediation as socially situated within collective dynamics shaping adoption and practice. Peer environments influence implementation of protective behaviors, while informal networks function both as barriers and diffusion channels [29]. Participation structures vary between parent-only and joint parent–child engagement, with many studies describing parents as co-learners rather than sole instructors [11, 30]. Interaction with existing family authority structures and expertise distributions is also documented [1, 3]. Some approaches rely on external facilitators guiding interaction [53], whereas others embed facilitation within collaborative systems [46].

4.4.2 Designing Learning in Privacy Support

Research portrays learning design as responding to heterogeneous family conditions rather than assuming uniform learners. Studies document developmental shifts motivating differentiated learning structures aligned with evolving parental roles and child autonomy [28, 54]. Some approaches frame privacy learning as ongoing developmental adaptation rather than a single instructional event [16]. Learning activities are frequently described as progressive and differentiated, incorporating incremental challenges, parallel learning tracks, and adaptation to varying literacy levels [11, 28, 46]. These approaches position privacy learning as cumulative and individualized. Variation also reflects differing mediation philosophies, ranging from collaborative exploration to rule-based guidance [23, 27]. Across studies, learning design emerges as a primary source of variation shaping how families engage with privacy support.

4.4.3 Communication and Engagement in Privacy Support

Research describes communicative and experiential design elements as central mechanisms through which privacy support becomes accessible and engaging. Privacy concepts are frequently portrayed as difficult to grasp when presented abstractly, motivating approaches grounded in relatable everyday contexts [4, 30, 53]. Narrative and scenario-based framing emerges as a recurring strategy translating abstract risks into recognizable experiences [11, 18, 46]. Facilitation-based formats structure engagement through guided discussion and conversational scaffolds [4, 53]. Tangible artifacts and visualizations materialize otherwise invisible data practices, enabling shared interpretation [30, 50]. Interactive participation formats such as games and hands-on environments are described as supporting active engagement and discussion [30, 46, 50]. Studies further describe variation in emotional framing, ranging from risk-oriented messaging to playful or facilitative approaches designed to reduce discomfort and sustain participation [11, 18, 28, 53]. Across this body of work, communication and engagement are characterized as design dimensions shaping how families experience and remain involved in privacy learning over time.

5 Coverage and Gaps in Existing Interventions

5.1 Overview of Interventions

The corpus includes seven evaluated interventions plus one design proposal that address parental privacy and cybersecurity support through three broad approaches: structured educational programs targeting parents as individual learners, facilitated formats engaging parent–child dyads through guided activities or institutional settings, and parental-control approaches for restructuring oversight.

Educational programs. Chen et al. [11] developed a six-episode video curriculum delivered to parents over 14 weeks, covering security and privacy basics, platform-specific risks, and strategies for supporting adolescents in navigating these online. Grounded in motivation theory, the program was evaluated through a randomized controlled trial measuring changes in parental security awareness, self-efficacy, and internet-specific mediation behavior across four sub-dimensions. Flores et al. [18] addressed a Spanish-speaking audience in Ecuador through a Moodle-based virtual learning environment combining video content, gamified activities, and 3D-animated scenarios across four cybersecurity modules. The platform targeted a joint audience of children, parents, and teachers, with learning outcomes assessed through pre/post module quizzes and platform performance metrics.

Facilitated family interaction. Wen et al. [53] facilitated two-hour sessions with parent-child dyads using structured perspective-taking exercises, with the aim of shifting privacy conversations away from one-directional instruction toward collaborative interpretation. The study identified three recurring communication patterns impeding productive dialogue: abstract framing, reliance on absolute statements, and declining adolescent engagement, and examined how the facilitation approach addressed these by drawing on children's own dig-

ital expertise. Liu et al. [30] contribute a design proposal rather than an evaluated artifact, positioning informal learning spaces such as museums and science centers as a largely untapped channel for family privacy education. Their analysis identifies four properties of these environments as particularly relevant: the quality family time they afford, the embodied experience of physical and interactive exhibits, their support for exploratory learning, and the lasting discussions they tend to prompt beyond the visit itself. Quayyum and Jaccheri [46] designed CyberFamily, a collaborative board game in which parent–child pairs work through scenario-based cybersecurity challenges using role-differentiated cards and narrative framing, inviting discussion without presupposing technical knowledge on either side. Wang et al. [50] developed the KOALA Hero Toolkit, combining a mobile tracker app with physical data cards and structured worksheets to make app-level datafication visible to families through investigation of their own devices. The toolkit positions critical questioning of data practices as the core activity rather than delivering content instructionally.

Parental control approaches. Akter et al. [2, 3] evaluated CO-oPS, an Android application enabling community members, including family groups, to share information about installed apps and permissions in support of collective privacy management. A four-week field study found increases in transparency, awareness, and self-efficacy across participants. A secondary analysis of the same dataset showed that self-efficacy gains were significantly stronger among caregivees than caregivers. Dumaru et al. [16] pursued a design critique approach by developing a low-fidelity prototype that reframes Google Family Link around open communication and child self-regulation rather than restriction. In a mixed-methods study comparing the redesign against the original interface, they examined whether shifting the framing of control mechanisms influences parents' mediation orientations. Parents rated the redesigned interface significantly higher across all three design principles, with the most pronounced effects for open communication features tied to YouTube activity and location monitoring.

5.2 Mapping Interventions to Criteria

Interventions were mapped against the design criteria framework to examine how support is distributed across learning outcomes and design features. While Table 2 presents an overview of the mapping, a detailed mapping is provided in Appendix A. The resulting mapping reveals structural regularities in how parental privacy support is operationalized across existing approaches and illustrates how empirical insights are reflected in implemented intervention designs, rather than detailing individual systems.

Within the reviewed interventions, implementation patterns most frequently concentrated on understanding of privacy risks, evaluative judgment, and parent–child communication, with nearly all interventions including awareness-oriented components and facilitating family dialogue [11, 16, 18, 30, 44, 50, 53]. Evaluative judgment appears frequently but typically as part of discussion- or scenario-based activities. In contrast, technical enactment and parental self-efficacy appear less consistently: procedural activities occur only in a subset of interventions [11, 18] and remain limited in scope, while confidence or agency development is rarely articulated as a primary learning objective.

Implementation patterns similarly cluster across design features. Interventions predominantly rely on joint parent–child participation and engagement-oriented communication formats such as relatable scenarios, interactive activities, and narrative framing. Most also employ structured facilitation, i.e. defined activity sequences, guided tasks, or phased session designs, though explicit curriculum-style learning progressions are limited to a smaller subset [11, 18].

Overall, the reviewed interventions suggest a convergence around awareness-building, collaborative discussion, and engagement-focused learning formats while operationalizing procedural and capability-oriented components more selectively. Rather than combining criteria uniformly, interventions emphasize recurring constellations of support: some foreground conceptual understanding through structured explanation, others center reflective dialogue and joint interpretation, and a smaller subset engages families directly in procedural interaction with privacy tools or settings. These distributions describe how interventions are currently realized and motivate closer examination of areas that remain comparatively underrepresented within the design space.

5.3 Conceptual-Operational Gaps and Structural Blind Spots

Comparing intervention implementations with empirical findings suggests differences in how identified parental needs are translated into operational support. While prior work positions privacy mediation as shaped by contextual interpretation, relational dynamics, and evolving family practices, implementations tend to instantiate these needs through bounded learning formats and structured activities. Understanding of privacy risks is widely addressed, yet operationalization primarily emphasizes structured knowledge acquisition. Implementations emphasize recognition and explanation of risks and data practices, whereas literature findings position understanding as meaningful mainly when applied within ongoing everyday decision-making contexts [1, 11, 18, 29, 30, 46, 50, 53]. A similar translation pattern appears for evaluative judgment. Although prior work positions evaluation as an ongoing interpretive capability emerging through lived experience, interventions operationalize reflection mainly as episodic activities embedded in learning sessions or omit explicit scaffolding altogether [29, 50, 54]. Technical enactment was addressed less consistently across interventions. While empirical research

Table 2: Mapping of evaluated intervention studies to design criteria dimensions. Filled circles indicate that a study addresses the respective criterion; empty circles indicate it does not. Studies are grouped by intervention type.

	Learning Outcomes					Design Features		
	Under-standing	Evaluative judgment	Technical skills	Self-efficacy	Parent–child commun.	Organi-zation	Designing learning	Comm. & engagement
Educational Programs								
Chen et al. [11]	●	●	●	●	●	●	●	●
Flores et al. [18]	●	○	●	○	●	●	●	●
Facilitated Family Interaction								
Wen et al. [53]	●	●	○	○	●	●	●	●
Liu et al. [31] *	●	●	○	○	●	●	●	●
Quayyum & Jaccheri [44]	●	●	○	○	●	●	●	●
Wang et al. [50]	●	●	○	●	●	●	●	●
Parental Control Approaches								
Dumaru et al. [16]	○	○	●	●	●	●	○	●
Akter et al. [2, 3]	○	●	●	●	○	●	○	●

● criterion addressed ○ not addressed * design proposal

positions procedural competence as necessary for translating privacy intentions into action, implementation practice frequently prioritizes awareness and discussion, with only a subset enabling direct configuration or hands-on interaction with privacy controls [2, 3, 11, 16, 18, 27–29]. Parental self-efficacy follows a comparable pattern. Prior work positions perceived capability and legitimacy to act as key determinants of engagement, yet implementation practice rarely operationalizes confidence-building explicitly. Where agency support appears, it emerges indirectly through collaborative interaction or system design rather than dedicated learning mechanisms [50, 54], with [11] as a notable exception. In contrast, parent-child privacy communication shows closer alignment between knowledge and implementation. Both literature and intervention practice emphasize dialogue, joint interpretation, and collaborative reasoning grounded in everyday situations, although implementations typically situate these interactions within bounded intervention encounters rather than sustained family practices [11, 18, 30, 46, 50, 53].

Translation differences also appear across design-feature criteria. While prior work positions privacy support as socially embedded across institutional and community contexts, implementations predominantly organize participation through artifact-centered parent-child activities with limited sustained organizational embedding, except [18] (schools) and [30] (museum). Likewise, adaptive learning described in the literature is operationalized primarily through structured progression and guided practice within predefined learning environments. Communication and engagement design shows stronger correspondence, as both literature and implementation consistently rely on relatable contexts, interactive participation, and experiential framing to support engagement [2, 3, 11, 16, 18, 30, 46, 50, 53].

Several dimensions remain sparsely represented across intervention formats, indicating structural blind spots rather than isolated limitations of individual approaches. Across the reviewed studies, a consistent pattern emerges in which interventions privilege awareness-building, communicative engagement, and structured learning activities, while underemphasizing sustained institutional embedding, reflective practice as an ongoing process, and explicit mechanisms for strengthening parental self-efficacy. Taken together, this reflects a design logic oriented toward bounded, session-based learning and short-term engagement, where privacy support is primarily enacted through discrete activities rather than embedded, longitudinal capability formation within family and institutional contexts.

6 Discussion

6.1 Design Space Dynamics

The design criteria framework and mapping presented in Section 4 and Section 5 reveal a fragmented but patterned landscape of parental privacy support. Rather than reflecting isolated design decisions, the observed concentrations and gaps suggest recurring tensions shaping how support is conceptualized and operationalized. The discussion interprets these structural patterns by considering broader dynamics emerging across research strands.

6.1.1 Supporting Action Without Oversimplifying

Privacy and cybersecurity challenges in family contexts are inherently complex and situational. Parents navigate evolving platforms, conflicting norms, and uncertain consequences, often relying on contextual judgment rather than fixed rules [4, 27, 30, 39]. Interventions widely respond to this complexity by prioritizing accessibility and lowering barriers to engagement

through narrative framing, relatable scenarios, and awareness-oriented instruction.

Yet this emphasis on accessibility comes at a cost. The gap analysis shows that while conceptual understanding is broadly addressed, evaluative judgment remains comparatively thin. Where reflection appears, it tends to be episodic rather than a skill families can draw on independently [30,53]. Importantly, the empirical literature consistently positions evaluative judgment, rather than awareness alone, as what enables families to act on privacy challenges [4, 39]. As a result, interventions risk providing a surface-level understanding of privacy and cybersecurity issues while falling short of fostering the deeper capacity to reason through unfamiliar privacy dilemmas and make informed decisions in future, unanticipated contexts.

6.1.2 Individual Responsibility Within Distributed Family Expertise

A second recurring dynamic concerns how responsibility and expertise are distributed within families. Much prior work implicitly assumes parents as primary decision-makers responsible for managing children's digital privacy and security. However, empirical studies repeatedly describe situations in which children possess greater platform familiarity or technical knowledge, creating asymmetries that challenge traditional models of parental authority [30,39,53]. The framework highlights the prominence of parent–child communication as a learning outcome, with collaborative dialogue, joint interpretation, and negotiated decision-making suggesting a shift from unilateral mediation toward shared family sense-making. At the same time, parental self-efficacy remains comparatively less explicitly supported, indicating tensions between expectations of parental responsibility and the realities of distributed expertise. Interventions addressing these dynamics often structure participation to facilitate dialogue or shared reflection. While structured interaction can enable inclusive discussion, it may also introduce challenges related to autonomy and coordination, particularly as adolescents increasingly participate as active contributors rather than passive recipients of guidance. The resulting landscape reflects an ongoing transition from models centered on parental control toward approaches emphasizing collaborative mediation and negotiated privacy practices.

6.1.3 Scalability Constraints in Designing Support

The distribution of intervention designs further suggests a tension between scalability and depth of support. Many interventions adopt self-contained formats, such as short video series, digital tools, or game-based activities, that can be deployed with minimal facilitation and reach diverse audiences at relatively low cost [2,3,11,16,18,44,50]. While these approaches promote accessibility, they may offer fewer opportunities for sustained, experiential engagement with privacy practices and system behaviors. This limitation is particularly salient given that parents often report feeling overwhelmed by technical topics, highlighting the need for more guided support when navigating this aspect of privacy protection [27,28]. A similar trade-off emerges between immediate action and transferable competence: highly guided interventions can facilitate protective behaviors in the moment, whereas concept-focused approaches may foster broader reasoning skills without necessarily translating into practice. The comparatively limited presence of interventions that combine sustained support, experiential engagement, and scalable delivery suggests that balancing these objectives remains a central challenge within the current design space.

This challenge is compounded by the fact that privacy practices are socially embedded, shaped by institutional contexts, peer norms, and ongoing family dynamics [27, 28, 39, 53]. Supporting such processes often requires adaptation to developmental stages, literacy levels, or household circumstances. Facilitation-based or highly tailored interventions can accommodate these differences but are typically resource-intensive and difficult to scale. Standardized formats support broader dissemination while potentially reducing contextual responsiveness.

6.2 Understanding the Landscape of Parental Privacy Support

Taken together, the identified dynamics indicate that observed gaps in the intervention landscape do not merely reflect neglected topics but emerge from competing demands inherent to designing privacy support for families. Interventions repeatedly balance accessibility with complexity, authority with collaboration, and scalability with contextual adaptation. These tensions help explain why awareness-oriented and communication-focused approaches are widely represented, while procedural enactment, sustained organizational support, and explicit self-efficacy development remain less consistently operationalized. By organizing evidence across learning outcomes and design features, the framework makes these structural dynamics visible across previously disconnected strands of research. Viewing interventions collectively highlights how different approaches address similar challenges under varying constraints, revealing both areas of convergence and persistent limitations in how parental privacy and cybersecurity support has been realized to date. At the same time, these patterns illuminate characteristics of the broader research landscape. Across the corpus, formative and exploratory studies outnumber contributions evaluating concrete forms of support, leaving comparatively limited empirical evidence of how insights into parental needs and constraints translate into sustained intervention approaches. This imbalance suggests that the field remains in an intermediate stage of development in which problem articulation has progressed further than intervention validation. The comparatively thin in-

tervention evidence base observed in this review thus reflects not only a limitation of available work but also an empirical signal regarding the current maturity and orientation of research on parental privacy and cybersecurity support.

6.2.1 Contextualising the Framework

The framework can be situated within broader traditions of media literacy research (e.g. [21, 35, 36, 57]), which emphasise individuals' capacity to critically understand, navigate, and act within complex digital environments. Within these traditions, privacy and autonomy are typically conceptualised as capacities of individual learners. The parental interventions reviewed here, however, position parents simultaneously as learners, mediators, and proxy decision-makers, bearing responsibility for children's protection while navigating technological uncertainty, balancing safeguarding and autonomy, making decisions despite incomplete expertise, and maintaining trust within ongoing relationships.

Trepte et al.'s OPLIS framework [42], Kumar and Byrne's 5Ds framework [26], and Wang et al.'s Digital Autonomy framework [52] provide particularly useful lenses for interpreting the learning outcomes identified in our review. The learning outcomes align closely with established privacy literacy conceptualisations. Trepte et al.'s declarative/procedural distinction maps onto understanding privacy risks and enacting privacy-protective behaviours, while Kumar and Byrne's emphasis on evaluating information flows within social contexts corresponds closely to the reflective evaluation criterion. However, the transition from declarative understanding to procedural competence remains underoperationalised in the parental intervention landscape. Comparatively few interventions provide sustained opportunities to develop practical privacy skills, suggesting procedural competence is a distinct design challenge rather than an automatic outcome of increased knowledge.

Both OPLIS and the 5Ds framework focus primarily on individual learners, yet the interventions reviewed here point to additional requirements: parental self-efficacy, parent–child communication, and proxy decision-making on behalf of children. Supporting children's privacy therefore requires not only literacy development but also relational and caregiving capacities these frameworks address only indirectly.

A similar pattern emerges for digital autonomy. Engagement strategies identified in our framework—storytelling, gamification, scaffolding, and guided interaction—correspond closely to mechanisms in Wang et al. [52] and cybersecurity education research [59]. Yet these traditions focus on individual learners, whereas parental privacy support involves coordinating learning, decision-making, and responsibility across family members. Parental self-efficacy consequently emerges as a distinct consideration that is not explicitly foregrounded in child-autonomy frameworks.

Taken together, existing frameworks explain what privacy-literate or autonomous actors should know, evaluate, or do, while the present framework complements them by specifying the relational, organizational, and capability conditions under which such competencies can be developed and enacted within family life. Privacy support thus extends beyond knowledge and judgment to fostering confidence in parental roles, enabling negotiation with children, and supporting practical enactment across interdependent family roles. The framework thereby extends existing literacy and autonomy frameworks to account for the distinctive demands of parental privacy support, where learning, mediation, and caregiving responsibilities are deeply intertwined.

6.2.2 Operationalizing the Framework

The framework provides a structure for analyzing existing parental privacy interventions and reasoning about new intervention concepts. It can be applied to intervention concepts, prototypes, or implemented interventions. Researchers may use it retrospectively to analyze existing approaches or prospectively to inform the design of new forms of parental privacy support. The framework can be applied through four complementary steps: First, Table 1 can be used to identify relevant design dimensions. Researchers may begin by considering which intended learning outcomes their intervention seeks to support (e.g., understanding of privacy risks, technical enactment, parental self-efficacy) and which design features are envisioned for delivering that support. The representative aspects listed for each criterion provide a starting point for locating specific intervention objectives within the broader framework. Second, Figure 2 can be used to examine how similar dimensions have previously been operationalized. Once relevant criteria have been identified, the intervention mapping highlights existing studies that address comparable areas. This allows researchers to explore concrete examples of how particular learning outcomes or design features have been implemented and evaluated in prior work. Third, the gap analysis in Section 5 can be used diagnostically to situate a proposed intervention within the broader landscape. Researchers can assess whether their approach addresses dimensions that are already commonly represented or whether it engages comparatively underrepresented areas. The purpose of this comparison is not to privilege novelty over established approaches, but to support reflection on how a proposed intervention relates to existing patterns in the literature. Finally, the design space dynamics discussed in Section 6.1 can inform interpretation of design choices. The recurring tensions identified across the evidence base provide a lens for considering potential trade-offs associated with different intervention directions. Rather than prescribing particular solutions, these dynamics can help researchers articulate the assumptions and constraints shaping their design decisions.

Used in combination, the different elements of the framework provide a way to characterize interventions, compare

approaches, and situate new work within the existing landscape. As such, the framework can support both diagnostic and reflective use.

6.3 Limitations and Future Work

The scope of this SoK reflects boundaries inherent to the current state of research on parental privacy and cybersecurity interventions. The final corpus includes seven evaluated interventions plus one design proposal, which represents a comparatively small empirical base. This limited number means that individual studies strongly shape observed patterns and constrains the ability to identify stable design tendencies across intervention types. At the same time, the small intervention corpus constitutes an empirical observation in itself, indicating that translation from formative research on parental privacy into evaluated support approaches remains comparatively limited within the current research landscape. Likewise, the heterogeneity of study contexts, intervention formats, and evaluation approaches limits quantitative comparison while highlighting the diverse conditions under which parental privacy support is currently explored. The findings should also be interpreted in light of methodological boundaries inherent to qualitative evidence synthesis. Although the literature identification followed a systematic procedure, relevant work may exist outside the selected venues or disciplinary keywords due to the interdisciplinary nature of family privacy research. In addition, the design criteria framework represents an analytic abstraction derived from recurring patterns across studies rather than an exhaustive taxonomy of possible intervention characteristics. The framework therefore supports comparative interpretation of existing work but does not claim to capture all potential forms of parental privacy support.

These limitations point to concrete directions for future research. Addressing the observed emphasis on awareness over enactment may require longitudinal investigations of how parental capabilities develop beyond short-term outcomes. The distributed nature of family expertise suggests opportunities for formats explicitly supporting collaborative learning and shared decision-making. More broadly, advancing this area may depend on reconciling context-sensitive family practices with scalable support structures, reflecting the tensions between simplification, participation, and sustainability discussed in Section 6.1. These directions reflect challenges inherent in translating empirical knowledge into sustainable intervention designs.

7 Conclusion

This paper systematized research on parental privacy and cybersecurity support by synthesizing evidence across prestudies, evaluated interventions, and related work on parental control technologies. The resulting design criteria framework distinguishes between intended learning outcomes and the design features through which privacy support is operationalized, enabling comparison across previously fragmented strands of research. Applying this framework highlighted recurring concentrations and absences within the existing intervention landscape. The reviewed interventions predominantly emphasize awareness-building, communication, and engagement-oriented learning formats, while procedural enactment, sustained organizational support, and explicit development of parental self-efficacy remain comparatively less operationalized. Rather than reflecting isolated design choices, these distributions may reflect broader structural conditions shaping how parental privacy support is translated from empirical knowledge into implemented interventions. By organizing heterogeneous evidence within a shared analytical lens, this SoK provides an interpretive account of the emerging design space for parental privacy and cybersecurity interventions. The framework functions as a diagnostic structure that makes visible how different approaches address similar challenges under varying constraints, clarifying areas of convergence as well as persistent translation gaps across the literature. In doing so, the paper contributes a clearer understanding of the current maturity and orientation of research on parental privacy support, offering a foundation for cumulative investigation of how families can be supported in navigating privacy and cybersecurity challenges.

Ethic Statement

This paper synthesizes previously published research and involves no new data collection or human participants. No institutional ethics approval was required. We are committed to representing prior work accurately and acknowledge limitations and potential biases in our synthesis where relevant.

Acknowledgments

References

[1] Mamtaj Akter, Amy J. Godfrey, Jess Kropczynski, Heather R. Lipford, and Pamela J. Wisniewski. From Parental Control to Joint Family Oversight: Can Parents and Teens Manage Mobile Online Safety and Privacy as Equals? *Proc. ACM Hum.-Comput. Interact.*, 6(CSCW1):57:1–57:28, April 2022.

[2] Mamtaj Akter, Jess Kropczynski, Heather Lipford, and Pamela Wisniewski. Examining Caregiving Roles to Differentiate the Effects of Using a Mobile App for Community Oversight for Privacy and Security. *Proceedings on Privacy Enhancing Technologies*, 2025.

[3] Mamtaj Akter, Madiha Tabassum, Nazmus Sakib Miazi, Leena Alghamdi, Jess Kropczynski, Pamela J. Wis-

niewski, and Heather Lipford. Evaluating the Impact of Community Oversight for Managing Mobile Privacy and Security. pages 437–456, 2023.

[4] Kenan Kamel A Alghythee, Adel Hrncic, Karthik Singh, Sumanth Kunisetty, Yaxing Yao, and Nikita Soni. Towards Understanding Family Privacy and Security Literacy Conversations at Home: Design Implications for Privacy Literacy Interfaces. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, CHI '24, pages 1–12, New York, NY, USA, May 2024. Association for Computing Machinery.

[5] Mary Jean Amon, Nika Kartvelishvili, Bennett I. Bertenthal, Kurt Hugenberg, and Apu Kapadia. 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):116:1–116:30, April 2022.

[6] Mohamed Ayyash, Tariq Alsboui, Omar Alshaikh, Isa Inuwa-Dutse, Saad Khan, and Simon Parkinson. Cybersecurity Education and Awareness Among Parents and Teachers: A Survey of Bahrain. *IEEE Access*, 12:86596–86617, 2024.

[7] Veronica Barassi. The Child as Datafied Citizen: Critical Questions on Data Justice in Family Life. In Giovanna Mascheroni, Anna Jorge, and Cristina Ponte, editors, *Digital Parenting: The Challenges for Families in the Digital Age*, pages 169–177. NORDICOM, Gothenburg, November 2018.

[8] European Data Protection Board. Record fine for Instagram following EDPB intervention. Technical report, September 2022.

[9] Rita Brito and Patrícia Dias. "Which apps are good for my children?": How the parents of young children select apps. *International Journal of Child-Computer Interaction*, 26:100188, 2020.

[10] Hongliang Chen, Christopher E. Beaudoin, and Traci Hong. Teen online information disclosure: Empirical testing of a protection motivation and social capital model. *Journal of the Association for Information Science & Technology*, 67(12):2871–2881, December 2016.

[11] Xiaowei Chen, Verena Distler, Chloe Gordon, Yaxing Yao, and Ziwen Teuber. Empowering Parents to Support Children's Online Security and Privacy: Findings from a Randomized Controlled Trial. In *Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security*, CCS '25, pages 1934–1948, New York, NY, USA, November 2025. Association for Computing Machinery.

[12] Chhaya Chouhan, Christy M. LaPerriere, Zaina Aljallad, Jess Kropczynski, Heather Lipford, and Pamela J. Wisniewski. Co-designing for Community Oversight: Helping People Make Privacy and Security Decisions Together. *Proc. ACM Hum.-Comput. Interact.*, 3(CSCW):146:1–146:31, November 2019.

[13] Irish Data Protection Commission. Irish Data Protection Commission announces €345 million fine of TikTok. Technical report, September 2023.

[14] Irish Data Protection Commission. Irish Data Protection Commission fines Meta €251 million. Technical report, December 2024.

[15] Laurien Desimpelaere, Liselot Hudders, and Dieneke Van de Sompel. Children's and Parents' Perceptions of Online Commercial Data Practices: A Qualitative Study. *Media and Communication*, 8(4):163–174, November 2020. Number: 4.

[16] Prakriti Dumaru, Hanieh Atashpanjeh, and Mahdi Nasrullah Al-Ameen. "It's hard for him to make choices sometimes and he needs guidance": Re-orienting Parental Control for Children. *Proc. ACM Hum.-Comput. Interact.*, 8(CSCW1):82:1–82:51, April 2024.

[17] Álvaro Feal, Paolo Calciati, Narseo Vallina-Rodriguez, Carmela Troncoso, and Alessandra Gorla. Angel or Devil? A Privacy Study of Mobile Parental Control Apps. In *Proceedings of Privacy Enhancing Technologies (PoPETS)*, volume 2020, Montreal, Canada, July 2020.

[18] Denys A. Flores, David Cruz, Stacy L. Cannon, Hugo Moncayo, Pablo Del Hierro, and Julián Galindo-Losada. A SCRUM-based Methodology for Implementing an Interactive Virtual Learning Environment to Teach Cybersecurity to Children. In *2023 XLIX Latin American Computer Conference (CLEI)*, pages 1–10, October 2023.

[19] Terese Glatz, Elizabeth Crowe, and Christy M. Buchanan. Internet-specific parental self-efficacy: Developmental differences and links to Internet-specific mediation. *Computers in Human Behavior*, 84:8–17, July 2018.

[20] Vahiny Gnanasekaran and Katrien De Moor. Providing user perspectives to the next generation of parental controls. *International Journal of Child-Computer Interaction*, 44:100735, June 2025.

[21] Shayl F. Griffith, Katie C. Hart, Samantha M. Casanova, Allison C. Goodman, Jenny S. Radesky, Rex Forehand, and Daniel M. Bagner. Promoting Healthy Screen Media Use in Young Children With Externalizing Behavior

Problems Through an Adapted Parenting Intervention: Results of an Open Trial. *Cognitive and Behavioral Practice*, 32(3):430–442, August 2025.

[22] Moritz Gruber, Christian Höfig, Maximilian Golla, Tobias Urban, and Matteo Große-Kampmann. "We may share the number of diaper changes": A Privacy and Security Analysis of Mobile Child Care Applications. *Proceedings on Privacy Enhancing Technologies*, 3:394–414, 2022.

[23] Syahida Hassan, Rahayu Ahmad, Alawiyah Abd Wahab, Fathey Mohammed, and Ayi Purbasari. Parental Strategies for Mitigating Online Threats and Enhancing Children's Cybersecurity Awareness. *Journal of Information and Communication Technology*, 24(4):111–134, October 2025.

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

[25] Priya Kumar and Sarita Schoenebeck. 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*, CSCW '15, pages 1302–1312, New York, NY, USA, 2015. Association for Computing Machinery.

[26] Priya C. Kumar and Virginia L. Byrne. The 5Ds of privacy literacy: a framework for privacy education. *Information and Learning Sciences*, 123(7/8):445–461, August 2022.

[27] Ann-Kristin Lieberknecht. Exploring determinants of parental engagement in online privacy protection: A qualitative approach. In *Proceedings of the 2024 European Symposium on Usable Security*, EuroUSEC '24, page 94–111, New York, NY, USA, 2024. Association for Computing Machinery.

[28] Ann-Kristin Lieberknecht, Sascha Löbner, and Frédéric Tronnier. 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, New York, NY, USA, 2026. Association for Computing Machinery.

[29] Ann-Kristin Lieberknecht and Aline Melanie Ochs. Safeguarding Children's Digital Privacy: Exploring Design Requirements for Effective Literacy Training for Parents. In Lynette Drevin, Wai Sze Leung, and Suné von Solms, editors, *Information Security Education - Challenges in the Digital Age*, pages 111–126, Cham, 2024. Springer Nature Switzerland.

[30] Lanjing Liu, Lan Gao, Nikita Soni, and Yaxing Yao. Exploring Design Opportunities for Family-Based Privacy Education in Informal Learning Spaces. *Proceedings on Privacy Enhancing Technologies*, 2024.

[31] Lanjing Liu, Lan Gao, and Yaxing Yao. Integrating Family Privacy Education and Informal Learning Spaces: Characteristics, Challenges and Design Opportunities. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems*, CHI EA '24, pages 1–9, New York, NY, USA, May 2024. Association for Computing Machinery.

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

[33] Sonia Livingstone, Leslie Haddon, Anke Görzig, and Kjartan Ólafsson. 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, 2011. Num Pages: 159 Place: London, UK Publisher: EU Kids Online, The London School of Economics and Political Science.

[34] Sonia Livingstone and Ellen J. Helsper. Parental Mediation of Children's Internet Use. *Journal of Broadcasting & Electronic Media*, 52(4):581–599, November 2008.

[35] Sonia Livingstone, Giovanna Mascheroni, and Mariya Stoilova. The outcomes of gaining digital skills for young people's lives and wellbeing: A systematic evidence review. *New Media & Society*, 25(5):1176–1202, May 2023.

[36] Duri Long and Brian Magerko. What is AI Literacy? Competencies and Design Considerations. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI '20, pages 1–16, New York, NY, USA, April 2020. Association for Computing Machinery.

[37] Renkai Ma, Dominique Geissler, Stefan Feuerriegel, Tobias Lauinger, Damon McCoy, and Pamela J. Wisniewski. Analyzing Social Media Claims regarding Youth Online Safety Features to Identify Problem Areas and Communication Gaps. *Proceedings of the ACM on Human-Computer Interaction*, 10(2):CSCW005:1–31, May 2026.

[38] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. Reliability and Inter-rater Reliability in Qualitative Research: Norms and Guidelines for CSCW and HCI Practice. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW):72:1–72:23, November 2019.

[39] Kate Muir and Adam Joinson. An exploratory study into the negotiation of cyber-security within the family home. *Frontiers in Psychology*, 11, March 2020.

[40] Peter Nikken and Marjon Schols. How and Why Parents Guide the Media Use of Young Children. *Journal of Child and Family Studies*, 24(11):3423–3435, 2015.

[41] Matthew J Page, Joanne E McKenzie, Patrick M Bossuyt, Isabelle Boutron, Tammy C Hoffmann, Cynthia D Mulrow, Larissa Shamseer, Jennifer M Tetzlaff, Elie A Akl, Sue E Brennan, et al. The prisma 2020 statement: an updated guideline for reporting systematic reviews. *bmj*, 372, 2021.

[42] Jinkyung Katie Park, Mamtaj Akter, Pamela Wisniewski, and Karla Badillo-Urquiola. It's Still Complicated: From Privacy-Invasive Parental Control to Teen-Centric Solutions for Digital Resilience. *IEEE Security & Privacy*, 22(5):52–62, September 2024.

[43] Sandra Petronio. *Boundaries of privacy: Dialectics of disclosure*. Suny Press, 2002.

[44] Farzana Quayyum. Collaboration between parents and children to raise cybersecurity awareness. In *European Interdisciplinary Cybersecurity Conference*, pages 149–152, Stavanger Norway, June 2023. ACM.

[45] Farzana Quayyum and Letizia Jaccheri. *An exploratory study about the role of gender in cybersecurity awareness for children*. IADIS Press, 2023. 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.

[46] Farzana Quayyum and Letizia Jaccheri. CyberFamily: A collaborative family game to increase children's cybersecurity awareness. *Entertainment Computing*, 52:100826, January 2025.

[47] Irwin Reyes, Primal Wijesekera, Joel Reardon, Amit Elazari Bar On, Abbas Razaghpanah, Narseo Vallina-Rodriguez, and Serge Egelman. "Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale. Barcelona, Spain, July 2018.

[48] Gisela Schubert and Susanne Eggert. "Daddy, Your Mobile is Stupid, you should Put it Away": Media Education from the Perspective of Professionals. In Giovanna Mascheroni, Cristina Ponte, and Ana Jorge, editors, *Digital parenting: the challenges for families in the digital age*, pages 147–156. Nordicom, Göteborg, 2018.

[49] Natalija Vlajic, Marmara El Masri, Gianluigi M. Riva, Marguerite Barry, and Derek Doran. 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, pages 96–103, New York, NY, USA, January 2018. Association for Computing Machinery.

[50] Ge Wang, Jun Zhao, Konrad Kollnig, Adrien Zier, Blanche Duron, Zhilin Zhang, Max Van Kleek, and Nigel Shadbolt. KOALA Hero Toolkit: A New Approach to Inform Families of Mobile Datafication Risks. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, CHI '24, pages 1–18, New York, NY, USA, May 2024. Association for Computing Machinery.

[51] Ge Wang, Jun Zhao, Max Van Kleek, and Nigel Shadbolt. Protection or Punishment? Relating the Design Space of Parental Control Apps and Perceptions about Them to Support Parenting for Online Safety. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW2):343:1–343:26, October 2021.

[52] Ge Wang, Jun Zhao, Max Van Kleek, and Nigel Shadbolt. 12 Ways to Empower: Designing for Children's Digital Autonomy. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, CHI '23, pages 1–27, New York, NY, USA, April 2023. Association for Computing Machinery.

[53] Zikai Wen, Lanjing Liu, and Yaxing Yao. Supporting Family Discussions About Digital Privacy Through Perspective-Taking: An Empirical Investigation. In *2025 IEEE Symposium on Security and Privacy (SP)*, pages 1288–1305, May 2025. ISSN: 2375-1207.

[54] Olivia Williams, Yee-Yin Choong, and Kerrianne Buchanan. Youth understandings of online privacy and security: A dyadic study of children and their parents. In *In Proceedings of the Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023). USENIX Association*, pages 399–416, 2023.

[55] Pamela Wisniewski, Arup Kumar Ghosh, Heng Xu, Mary Beth Rosson, and John M. Carroll. 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, pages 51–69, New York, NY, USA, February 2017. Association for Computing Machinery.

[56] Pamela Wisniewski, Haiyan Jia, Heng Xu, Mary Beth Rosson, and John M. Carroll. "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, pages 302–316, New York, NY, USA, 2015. Association for Computing Machinery.

[57] Maryna Yachmenyk, Inna Kharchenko, Olena Semenog, Mariia Ostroha, Serhiy Petrenko, Vitaliy Dubinsky, and Olena Semenikhina. Development of Information and Media Literacy in the System "Students-Parents-Teachers": Ukrainian Practice. In *2024 47th MIPRO ICT and Electronics Convention (MIPRO)*, pages 430–435, May 2024.

[58] Maggie Zgambo, Edah Anyango, Diana H. Arabiat, Irene Ngune, Evalotte Mörelius, Min Zhang, and Lisa Claire Whitehead. Effect of Digital Safety Interventions on Parental Practices in Safeguarding Children's Digital Activities: Systematic Review and Meta-Analysis. *JMIR pediatrics and parenting*, 8:e70745, October 2025.

[59] Leah Zhang-Kennedy and Sonia Chiasson. A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education. *ACM Computing Surveys*, 54(1):12:1–12:39, January 2021.

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

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

[62] Wenxin Zhao, Fangyu Yu, Peng Zhang, Hansu Gu, Lin Wang, Siyuan Qiao, Tun Lu, and Ning Gu. YouthCare: Building a Personalized Collaborative Video Censorship Tool to Support Parent-Child Joint Media Engagement. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, CHI '25, pages 1–20, New York, NY, USA, April 2025. Association for Computing Machinery.

A Appendix

Ref.	Understanding	Reflection	Technical	Self-Efficacy	Parent–Child Communication	Organization	Designing Learning	Communication & Engagement
[11]	Conceptual S&P overview; app risks; monitoring tools; consequences framing; family dialogue; emerging AI-related risks	Self-reflection on practices; everyday privacy decision-making	Privacy setting configuration; tool-based privacy control; guided technical walkthrough	Internet-specific parenting self-efficacy; guided competence development	Open privacy dialogue; negotiation of privacy decisions	Parent-only participation; artefact-guided interaction	Structured learning progression; guided practice activities	Narrative or scenario framing; relatable everyday contexts; tangible or visual representations; emotionally moderated framing
[18]	Internet threats (bullying, grooming, sexting, identity theft); social engineering tactics; monitoring and safe navigation; legal response and family communication; platform-related risks (social media, games, mobile)	/	Privacy setting configuration; permission and access management	/	Open family dialogue; effective intra-family communication	Joint parent–teacher–child participation; artefact-guided interaction	Structured learning progression	Playful or gamified engagement; emotionally moderated framing; tangible or visual representations
[30]	Interactive data-flow visualization (third-party tracking); teachable moments in contextual scenarios; foundational concepts (consent, norms, information flow) *(proposed)*	Everyday privacy decision-making; critical data ecosystem reflection	/	/	Open family dialogue; joint privacy interpretation; ongoing privacy discussions	Joint parent–child participation; institutionally embedded support; artefact-guided interaction *(proposed)*	Guided practice activities; developmentally adapted learning	Relatable everyday contexts; interactive engagement formats; tangible or visual representations; playful or gamified engagement
[53]	Perspective-taking on data needs and privacy concerns; categorization of data types (transparency, conditional, private); privacy as spectrum; mental models of data-sharing trade-offs	Self-reflection on practices; perspective comparison; everyday privacy decision-making	/	/	Joint privacy interpretation; perspective-taking dialogue; negotiation of privacy decisions	Joint parent–child participation; facilitated support structure	Structured learning progression; guided practice activities; parallel or differentiated learning paths	Relatable everyday contexts; interactive engagement formats; emotionally moderated framing

Ref.	Understanding	Reflection	Technical	Self-Efficacy	Parent–Child Communication	Organization	Designing Learning	Communication & Engagement
[46]	Scenario-based cybersecurity risks (social media privacy, phishing, passwords, cyberbullying); behavioral reflection in everyday situations; cybersecurity knowledge transfer within families	Everyday privacy decision-making; contextual risk evaluation; self-reflection on practices	/	/	Reciprocal parent–child learning; joint privacy interpretation; guided parent–child reflection	Joint parent–child participation; artefact-guided interaction	Structured learning progression; developmentally adapted learning; guided practice activities; parallel or differentiated learning paths	Narrative or scenario framing; relatable everyday contexts; interactive engagement formats; playful or gamified engagement
[50]	Cognitive understanding of trackers and data types; situated reflection on app-specific data practices; linking abstract concepts to daily life; progression from basic awareness to critical questioning of data systems; awareness of data destinations and datafication risks	Self-reflection on practices; everyday privacy decision-making; contextual risk evaluation; critical data ecosystem reflection	/	Supported sense of agency; collaborative competence building	Joint privacy interpretation; negotiation of privacy decisions; reciprocal parent–child learning	Joint parent–child participation; artefact-guided interaction	Structured learning progression; guided practice activities; parallel or differentiated learning paths	Relatable everyday contexts; interactive engagement formats; tangible or visual representations; playful or gamified engagement
[16]	/	/	Sharing personal information; sharing location; sharing passwords	Adaptive parental role support	Fostering open communication; trust-building dialogue; encouragement of parent–child discussion	Parent-only participation; artefact-guided interaction	/	Relatable everyday contexts
[2]; [3]	/	Self-reflection on practices	App downloads; privacy permissions	Supported sense of agency	/	Joint parent–child participation; artefact-guided interaction	/	Relatable everyday contexts

Table 3: Classification of parent–child security and privacy interventions across learning and interaction dimensions.

Ref.	P/I	Study Design	Participants	Child Age	Country	Format/Tool	Duration/Sessions	Measurement Approach	Key Outcome Measure(s)
[1]	P	Semi-structured interviews; user study	19 parent-teen pairs	13–17	USA	CO-oPS Android app (community oversight of app permissions)	Single session (1–2.5 hrs); lab-based	Semi-structured interviews; think-aloud; guided tasks; qualitative thematic analysis	Perceived value of joint oversight; power dynamics; design recommendations for co-monitoring features
[3]	I	Mixed-methods longitudinal field study (survey, app logs, optional interviews)	22 self-formed groups of families, friends, co-workers (N=101, Android smartphone users)	Mixed (includes teens 13–17; majority 18–34)	USA	CO-oPS Android app (community oversight of app permissions + community feed)	4 weeks; weekly tasks + surveys	Pre/post surveys (Likert scales); app usage logs; optional semi-structured interviews; Wilcoxon rank-sum tests	Transparency, awareness, trust, individual/community participation, self-efficacy, community collective efficacy (all pre-post constructs)
[2]	I	Mixed-methods longitudinal field study (survey + app logs + interviews); secondary analysis differentiating caregivers vs caregivees	22 self-formed groups of families, friends, co-workers (N=101, Android smartphone users); N=51 caregivers, N=50 caregivees	Mixed (includes teens 13–17; majority 18–34)	USA	CO-oPS Android app	4 weeks	Pre/post surveys; app logs; interviews (N=51); 2x2 ART ANOVAs; Mann-Whitney U tests; qualitative coding	Differential effects on self-efficacy, community collective efficacy, community trust, belonging by caregiving role; app-hiding behavior
[4]	P	Qualitative; semi-structured interviews + design probe activity	13 Parents	<13; primarily 10–13	USA	no intervention tool; design probe using Common Sense Media webpage	Single session (20–59 min interviews)	Inductive thematic analysis; design probe activity	Five categories of parent-child privacy conversations; children's engagement patterns; design implications for privacy literacy interfaces
[11]	I	formative study (questionnaire) + main study RCT (2x2 pre/post, longitudinal); qualitative thematic analysis of open-ended feedback	Formative: N=210 Parents; Main RCT: N=201 Parents (N=88 intervention, N=113 control)	Grades 6–9	USA	Six short educational videos (∼29 min) on online S&P basics, digital parenting steps, parental monitoring, popular apps & risks, communication strategies, emerging risks	12-week intervention (6 episodes, one every 2 weeks); pre- and post-questionnaires	Generalized linear regression (pre/post); Wilcoxon signed-rank tests; t-tests for between-group comparisons; qualitative thematic analysis for open-ended feedback; validated Likert scales	Parental security awareness; parenting self-efficacy; parental concerns; internet-specific parental mediation; parental conversation approaches on S&P
[12]	P	community-based participatory design sessions + design artifacts	13 self-formed groups of families, friends, co-workers (N=32)	Mixed (teens to older adults; majority 18–34)	USA	Participatory co-design of a proposed CO-oPS mobile app concept (paper prototypes using 'Bags of Stuff' technique; scenario: MoviePass app privacy breach)	Single session (∼90 min); open co-design + feature introduction/redesign + presentation	Hybrid deductive (CO-oPS model: community, transparency, awareness, individual participation) + inductive open coding of video transcripts and design artifacts; iterative consensus coding	Translated CO-oPS model into design features (Expert Users, Discover, Activity Feed, App Scanner, Privacy Alerts, Sharing Mechanisms); identification of trust and active/passive participation as emergent themes; design recommendations for community-based privacy management
[16]	I	Qualitative design study + online survey (within-subject comparison)	22 self-formed groups of families, friends, co-workers (N=101, Android smartphone users);	5-12	USA	Low-fidelity Adobe XD prototype of redesigned Google Family Link; compared against Google Family Link baseline across 6 controls	Study 1: single session 30-60 min, virtual; Study 2: single session ∼15-20 min virtual	Study 1: inductive thematic analysis; Study 2: paired-sample t-test or Wilcoxon signed-rank; open-ended thematic coding	Perceived fostering of open communication (encouragement + support); instilling self-regulation (nudges toward/impact on future behavior); granularity (purpose-specific, content-based, trust-based) – treatment vs. baseline on 7-point Likert scales
[18]	I	Design & development study + evaluation	Needs analysis: N=745; Learning evaluation: N=24 (children + parents/teachers)	8-12	EC	Moodle-based interactive VLE; 4 modules with videos, games, 3D animated characters; Spanish-language; asynchronous + Zoom components	4 weeks; 5 notional hours/week (20 total)	Functional tests; load/stress tests; navigation task-completion timing; pre/post course quizzes per learning objective; descriptive frequency analysis	Cybersecurity knowledge gains across social engineering awareness, tool installation, grooming prevention, family communication; VLE platform performance; navigation experience
[20]	P	Semi-structured interviews + focus groups + pre-questionnaires	S1: multidisciplinary experts (N=5); S2: parents (N=6); S3: children + parents (N=14 + 14)	10-13	NO	No tool deployed	Interviews: 45-60 min each; Focus groups: ∼45 min each (4 sessions)	Empirically-close coding; pre-questionnaire data analyzed descriptively in Excel	Barriers/drivers in current parental controls for digital competence and cybersecurity awareness; design implications for next-generation parental controls (pedagogical features, nudging, autonomy-support, cultural adaptability, child co-design)
[23]	P	Semi-structured interviews	Parents whose children had experienced online threats (N=9)	not reported	MY	N/A (no intervention tool)	single session (30-60 min, virtual)	Semi-structured interviews; thematic analysis	Parental cyber-parenting styles (authoritative, authoritarian, permissive); coping strategies (problem-focused, emotion-focused); children's cybersecurity awareness
[27]	P	Semi-structured interviews with media educators	Media educators (N=8)	N/A	DE	N/A (no intervention tool)	Single session per educator; 50–70 min each	Semi-structured interviews; qualitative thematic analysis	Determinants of parental privacy protective behavior: socioeconomic status, age, gender, technical skills, self-efficacy, privacy awareness, privacy concern, social influence, parental emotions

P: Pre-Study I: Intervention *: Proposed

Ref.	P/I	Study Design	Participants	Child Age	Country	Format/Tool	Duration/Sessions	Measurement Approach	Key Outcome Measure(s)
[28]	P	Large-scale online survey; Partial Least Squares Structural Equation Modeling	G1: parents of children 6–11 yrs (N=498); G2: parents of children 12-15 yrs (N=502)	G1: 6–11 yrs; G2: 12–15 yrs	DE	N/A (no intervention tool)	Single online survey session (∼13 min)	Partial Least Squares Structural Equation Modeling	Parental privacy management behaviors: (1) child data disclosure regulation (sharenting), (2) parental privacy mediation, (3) regulation of others' sharing; antecedents: privacy concern, self-efficacy, technical skills, privacy knowledge, online engagement, peer influence, perceived overload
[29]	P	Semi-structured interviews with media educators and parents	Study I: media educators (N=8); Study II: parents (N=11)	0-5	DE	N/A (no intervention tool)	Study I: 50–70 min per interview	Semi-structured interviews; qualitative thematic analysis	Design requirements for effective privacy literacy training for parents; barriers to parental engagement; mismatches between educator and parental perspectives
[30]	I*	Semi-structured interviews	parent–child dyads (N=16)	6–14	USA	Informal learning spaces (museums, science centers, libraries) as proposed channel	interviews (23–59 min), virtual; single session	Semi-structured interviews; inductive thematic analysis; separate codebooks for parents and children	Current family privacy education practices; challenges (privacy tensions, complex contextual nature, knowledge gaps); design opportunities for ILS-based family privacy education
[39]	P	Exploratory, face-to-face semi-structured interviews	13 families (N=33, 14 parents + 19 children)	6–16	UK	N/A (no intervention tool)	Parent interviews ∼1 hour; child interviews 35–45 min; single visit per family	Semi-structured interviews; thematic analysis	Cybersecurity concerns (cyberbullying, stranger danger, privacy, content, financial scams, technical threats); management strategies (rules/boundaries, protective technology use, communication/education); family tensions over digital boundaries
[42]	I	Multiple embedded sub-studies (co-design, experimental, Youth Advisory Board)	Adolescents (ages 13–18); parents in referenced sub-studies; specific co-design participants aged 15–17	Adolescents (13–18 years)	USA	Locus (social media self-regulation app); online safety nudges; co-designed social media simulation; Youth Advisory Board (Discord + Zoom + Figma)	YAB: 1 year; Locus study: 2 weeks; ARC activities: 8 weeks	Multiple methods across sub-studies: pre/post surveys, exit interviews, Figma co-design sessions, asynchronous Discord discussions	Teen self-regulation (intentional media use, self-control); privacy autonomy; resilience; teen perceptions of social media privacy risks; nudge effectiveness and acceptability
[44]	I	Pilot study with low-fidelity game prototype + focus group discussions	parent–child pairs (N=8)	Children 9–12 years	NO	Collaborative maze board game (paper prototype); scenario-based cybersecurity challenges; color-coded cards for parents (yellow) and children (green)	Single game session + focus group; duration not reported	Focus group discussions post-game; qualitative; feasibility assessment; no formal learning outcome measure at this stage	Feasibility and acceptability of game concept; participant reactions; parent–child discussion quality
[45]	P	Explorativ, semi-structured interviews	Parents (N=25)	10–15	NO	N/A (no intervention tool)	Interviews 10–34 min; single session	Semi-structured interviews; thematic analysis	Parents' risk perceptions for children (5 categories: privacy, online content, online contact, online conduct, consumer risks); parental mediation strategies (active, restrictive, co-using); gender patterns in mediation and children's online activities
[50]	I	User study with hybrid toolkit (app + data cards + worksheets)	Families with school-age children (N=17, 23 children, 17 parents)	10-14	UK	KOALA Hero Toolkit: (1) Android mobile tracker app (built on TrackerControl), (2) data cards, (3) task sheet + worksheets	User study sessions; median 96 min per session	Qualitative user study; analysis of thought processes, perceptions, decision-making; families' critical thinking assessed qualitatively	Families' critical thinking about datafication risks; family engagement and discussion quality; perceptions of mobile app tracking; decision-making about app permissions
[53]	I	Structured facilitated sessions with parent–child dyads	parent–child pairs (N=26)	13–15	USA	Structured facilitation guide (perspective-taking theory); moderator-led discussion sessions; researcher field notes and participant worksheets	2-hour sessions per family; single session + post-session debrief	Constant comparative coding; thematic frequency described qualitatively	Communication patterns in family privacy discussions (abstract vs. concrete, absolute statements, teen disengagement); privacy literacy; shift from parent-led to collaborative discussion; perspective-taking effectiveness
[54]	P	Pre-interview questionnaires + semi-structured interviews	Youth (N=40); parents (N=40)	8–18	USA	N/A (no intervention tool)	Scheduled for 90 min per dyad (separate parent and child interviews); single session	Pre-interview questionnaire + semi-structured interviews; qualitative thematic analysis; constant comparative method	Youth knowledge of online privacy and security; parental strategies influencing youth knowledge (device monitoring, use-limiting, conversations); comparison across grade bands
[55]	I	Structured feature analysis of 75 Android mobile apps; value-sensitive design framework	No human participants	Adolescents (13–17 years; implied by app targets)	USA	75 Android parental control/online safety apps; analysis device: Google Nexus 5X	data collection during April–May 2016	Structured qualitative feature analysis; features mapped to conceptual framework	Feature distribution across TOSS categories; proportion of apps supporting each feature type; values embedded in app designs