

Closing the Protection Gap: From Insight to Intervention in Preventing Online Child Sexual Exploitation

Paper Submitted to ESOMAR Congress 2026

Authors:

Joy Ganvik, CEO, SA Market Insights

Anju Ahuja, COO and Co-Founder, Amplifyer

Date: September 2026

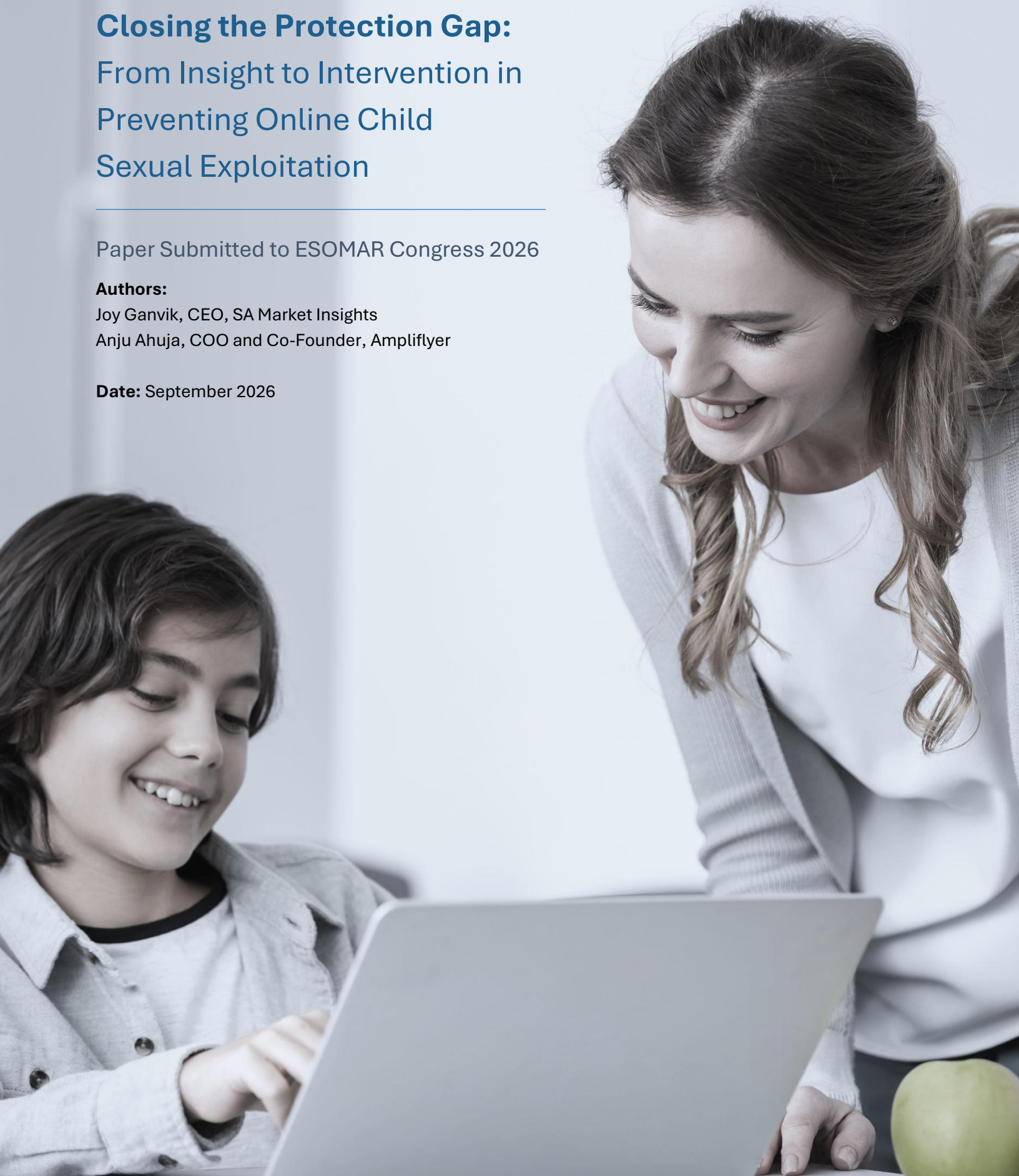


Table of Contents

Executive Summary	4
Introduction: Understanding the Protection Gap.....	6
Research Objectives	8
Methodology	10
Key Analytic Methodologies	11
AI-Enabled Intervention Development	14
Key Findings.....	16
Stakeholder Implications.....	37
Implications for the Research Industry	40
Ethical Considerations	41
Conclusion	43
References.....	44
Project Contributors	45
Appendix A: Sample Profile	46
Appendix B: Segmentation Methodology.....	48
Appendix C: MaxDiff Design	49
Appendix D: Driver Analysis Modeling Details	51
Appendix E: Example AI-Enabled Probing Flows	52
Appendix F: NLP-Assisted Verbatim Analysis	55
Appendix G: Example Amplifyer Intervention Concept.....	56
Appendix H: About SA Market Insights	57
Appendix I: About Amplifyer	58

Table of Figures

Figure 1: AI-Powered Adaptive Probing Process	11
Figure 2: NLP Assisted Verbatim Analysis Process	12
Figure 3: Types of Children's Risk Exposure.....	19
Figure 4: Verbatim Responses Related to Types of Children's Risk Exposure	19
Figure 5: Prioritization of Solutions – Probability of Choice	20
Figure 6: Probabilities of Choice	22
Figure 7: Segmentation Dimensions	23
Figure 8: Segmentation Dimensions: Variance From Average	24
Figure 9: Decision Factors for Solutions.....	26
Figure 10: Drivers of Preparedness	28
Figure 11: AI-Enabled Intervention for Pragmatic Balancers.....	23
Figure 12: AI-Enabled Intervention for Vigilant Managers	24
Figure 13: AI-Enabled Intervention for Social Risk Navigators	26
Figure 14: AI-Enabled Interventions for Engaged Protectors.....	28

Appendix

Figure A1: Sample Composition: Parent	46
Figure A2: Sample Composition: Household.....	46
Figure A3: Sample Composition: Children	47
Figure A4: Screenshot of MaxDiff Exercise	50
Figure A5: MaxDiff Cluster Solution - Differentiating Solutions.....	50
Figure A6: Verbatim Theme Comparison Pre and Post Smart Probe	55

Table of Tables

Table 1: Technical Guidance and Risk Mitigation Outputs	31
---	----

Appendix

Table A1: Fit Statistics.....	48
Table A2: Driver Analysis.....	51
Table A3: Revealing Specific Risks and Threat Perceptions.....	52
Table A4: Uncovering Parenting Philosophy and Trust Dynamics	53
Table A5: Identifying Practical Challenges and the “Protection Gap”	53
Table A6: Revealing How Children Interpret Online Safety Rules	54
Table A7: Surfacing Real Monitoring Behaviors and Safety Strategies	54

Executive Summary

Research Summary

Children today participate in a wider range of digital environments online than ever before, including social media, gaming, messaging, streaming, and connected digital environments. These digital technologies expose children to increasing online risks, including cyberbullying, exploitative interactions, scams, predatory grooming, and child sexual abuse material (CSAM).

This research develops actionable intervention strategies and objectively explores the growing “protection gap” between parental perceptions of online safety preparedness and the realities of children’s digital behaviors and risks. Findings are based on a national quantitative study conducted among US parents of children ages 6–17, designed to better understand parental concerns, safety behaviors, unmet needs, and barriers to intervention.

Beyond the substantive topic itself, the project also demonstrates how advanced research methodologies and AI-enabled approaches can help transform research from passive measurement into actionable intervention development. The study incorporates advanced quantitative methodologies including AI-powered adaptive probing, NLP-assisted verbatim analysis, latent class segmentation, MaxDiff prioritization modeling with cluster analysis, driver analysis modeling, and allocation-based trade-offs.

In addition, Amplifyer — an enterprise AI-native strategy and intelligence platform — was used to accelerate the translation of research findings into intervention concepts, communication frameworks, and actionable parent-support strategies. While Amplifyer’s platform is typically used by businesses to uncover market opportunities, develop disruptive products, and achieve growth, we saw an opportunity to leverage this unique platform for this investigation.

The findings reveal important disconnects between parental assumptions and children’s actual online experiences, highlight differing parent mindsets and protection approaches, and identify opportunities for technology companies, educators, policymakers, and child protection organizations to better support families. The challenge of protecting children is increased by the differing attitudes parents express as they examine tradeoffs between freedom of use and shielding children from possible harm. One size does not clearly fit all.

Ultimately, this paper illustrates how market research can evolve beyond insight generation toward enabling practical societal interventions that address different perceived needs in the population.

Key Findings and Implications

Parents widely recognize that children face meaningful online risks, but the findings reveal a substantial gap between awareness and effective protection in practice. While most parents report taking at least some steps to manage online safety, relatively few consistently use advanced monitoring tools, content filtering, or layered protection strategies. Many parents instead rely heavily on conversations, basic rules, or reactive intervention after issues arise. At the same time, parents report significant barriers to effective online safety management, including balancing privacy with monitoring, children resisting controls, uncertainty around which risks matter most, and difficulty keeping pace with evolving technologies and platforms. Together, these findings point to a growing “protection gap” between concern, preparedness, and sustained protective action.

The research also demonstrates that parents are not approaching online safety in a uniform way even relative to their perceived risks. Segmentation analysis identified four distinct parent mindsets, each reflecting different philosophies around perceived risks, monitoring, trust, communication, technology use, and intervention. Some parents take highly proactive and technology-driven approaches focused on monitoring and control, while others prioritize selective intervention, relationship dynamics, or maintaining balance between protection and independence. Importantly, these differences extend beyond simple concern levels and influence how parents evaluate online risks, what tools they adopt, how frequently they communicate with children, and which types of solutions they believe are most effective.

Across the study, parents consistently show the strongest interest in solutions that provide actionable protection and reduce the burden on parents themselves. Real-time alerts, parental controls, content filtering, privacy protection, and AI-enabled monitoring capabilities emerged as some of the highest-priority solutions, while communication-only or education-only approaches were viewed as less effective when used in isolation. At the same time, usage of many protective solutions remains relatively low despite high perceived importance, reinforcing the broader implementation gap identified throughout the research. The findings suggest that effective online safety strategies will likely require more than awareness campaigns alone, instead combining practical tools, communication support, trust-building approaches, and adaptive technologies that help parents translate concern into meaningful and sustainable action.

Author’s Note

Given the breadth and complexity of the topic, this paper is intentionally structured to support multiple levels of engagement. Because of the importance of the topic, we have chosen to provide depth of findings and methods rather than economizing on paper length. To that end, readers primarily interested in findings and implications may focus on the Executive Summary, Key Findings, Intervention Outputs and Stakeholder Implications sections, while those interested in methodological innovation and AI-assisted research workflows may explore the methodology and appendix sections in greater depth. Detailed examples, technical frameworks, and intervention outputs are included throughout the paper and appendices to provide transparency, illustrate the applied methodologies, and support practical interpretation of the findings.

Introduction: Understanding the Protection Gap

The Expanding Digital Reality for Children

Children today are growing up in a digital environment fundamentally different from previous generations. Social media, messaging applications, gaming ecosystems, livestreaming platforms, connected devices, and AI-enabled technologies have become embedded within children's everyday lives. Digital platforms increasingly influence how children communicate, learn, socialize, entertain themselves, and form relationships.

At the same time, these digital ecosystems expose children to a growing range of online safety risks. These risks include cyberbullying, inappropriate content exposure, scams and fraud, exploitative interactions, grooming behaviors, privacy violations, and child sexual abuse material (CSAM).

As online behaviors continue to evolve rapidly, parents and caregivers are increasingly expected to serve as the first line of defense in protecting children online. Yet many parents face significant challenges in understanding digital platforms, monitoring online interactions, balancing privacy and trust, and determining which protective actions are most appropriate or effective.

Defining the “Protection Gap”

This research centers around the concept of the “protection gap,” defined as the disconnect between:

- Parent perceptions of online safety preparedness
- Actual child digital behaviors and risks
- Parent confidence versus effective action
- Awareness of risks versus implementation of protections
- Available safety resources versus practical usability and adoption

This gap has important implications for families, educators, policymakers, technology companies, and child-protection organizations.

The Need for Action-Oriented Research

While awareness of online child safety concerns has grown substantially in recent years, much of the existing conversation remains focused on awareness rather than intervention.

Research often measures concerns, attitudes, or behaviors without providing practical pathways toward action. At the same time, organizations responsible for child safety frequently struggle to translate complex research findings into clear guidance, communication frameworks, intervention strategies, or usable tools for parents.

This project was designed not only to better understand the online safety ecosystem, but also to explore how advanced research methodologies and AI-enabled systems can accelerate the translation of insights into practical interventions.

Research Context and Relevance

This work was developed in the context of growing global concern around online child exploitation and broader online safety challenges. Many organizations are exploring, assessing, monitoring, and addressing the role of online methods in exploiting children to put protective measures in place and guide businesses and caregivers in how to better protect them.

Some of the key factors that led us to identify the need for this research which also influenced the research design, include:

- Research from Thorn, a nonprofit organization focused on technology-driven child protection and prevention of online child sexual exploitation, has demonstrated that exploitative interactions increasingly occur within mainstream digital environments rather than isolated platforms.
- Reports to NCMEC's CyberTipline increased substantially between 2021 and 2023, highlighting the growing scale and complexity of online child exploitation concerns; although overall report volume declined in 2024, some high-risk categories continue to rise.
- UNICEF has emphasized the need to balance child protection with digital inclusion, privacy, participation, and developmental opportunities.
- The Internet Watch Foundation has reported increasing volumes of online child sexual abuse material, including growing concerns around AI-generated exploitative imagery.
- The U.S. Surgeon General has emphasized that protecting youth online requires coordinated action across families, technology companies, policymakers, and researchers.
- Pew Research studies have shown that teens increasingly engage across multiple digital platforms simultaneously, creating more fragmented and difficult-to-monitor online experiences
- Ofcom research has highlighted the increasingly blurred boundaries between gaming, messaging, entertainment, and social interaction within children's digital lives.

Research Thesis

This paper reasons that:

1. Significant protection gaps exist between parent perceptions and children's digital realities
2. Parents require more practical, actionable support rather than awareness messaging alone
3. AI-driven research methodologies can:
 - provide deeper behavioral understanding (such as with adaptive probing) and
 - can also help accelerate the transformation of insights into practical interventions (using platforms like Amplifyer)
4. Market research can play a more active role in supporting societal outcomes beyond measurement

Research Objectives

The project was designed around four primary objectives.

1. Explore Digital Behaviors and Children's Online Risk Exposure

The first objective was to better understand how children engage with digital platforms and online ecosystems, including:

- Social media usage
- Messaging and communication behaviors
- Gaming interactions
- Streaming and content consumption
- Online relationship formation
- Device access and supervision realities
- Exposure to potentially risky interactions or content

The study sought to identify areas where parental assumptions may diverge from actual behaviors and experiences.

2. Understand Parent Mindsets, Concerns, and Protection Behaviors

The second objective focused on understanding how parents perceive online risks and how those perceptions influence protective behaviors.

Areas explored include:

- Perceived online risks
- Safety priorities
- Confidence in managing online safety
- Monitoring and supervision approaches
- Communication with children
- Privacy and trust dynamics
- Technology usage and safety tools
- Emotional barriers and uncertainties

3. Identify Unmet Needs and Opportunities for Intervention

The third objective focused on uncovering gaps within the broader online safety ecosystem; specifically:

- Areas where parents feel unsupported
- Gaps in education and communication
- Confusing or underutilized safety tools

- Opportunities for clearer guidance
- Intervention opportunities for organizations and stakeholders
- Differences in needs across parent segments

4. Demonstrate Advanced Methods and AI-Enabled Approaches

The project was designed to demonstrate how advanced market research approaches - including AI-assisted adaptive probing, NLP-supported analysis, and AI-enabled strategic intelligence systems, can support both:

- Deeper insight generation
- Faster translation of research findings into practical interventions

The project intentionally explored how research can move beyond passive reporting toward enabling actionable societal impact.

Methodology

Research Design Overview

The study consisted of a national quantitative online survey conducted among US parents. The target audience included parents or guardians of children ages 6–17 who have children living with them at least part time and play a role in approving or managing children’s online activities.

Sample Specifications – See Appendix A for more details.

Geography:	United States
Methodology:	Online quantitative survey
Sample Size:	n=1,014
Panel Provider:	InnovateMR
Fieldwork:	May 2026
Representation:	Representative demographically of US parents with children ages 6-17; no weighting

Survey Design and Content Areas

The questionnaire was designed to examine multiple dimensions of the online safety ecosystem.

Key Content Areas Included:

- Connected device and online usage (adults & children) across a range of platforms
- Parent awareness and concern levels
- Monitoring and supervision approaches, including the use of online safety tools
- Family trust and privacy dynamics
- Experiences with online incidents or risks
- Evaluation of safety features and tools
- Trade-offs between privacy, independence, and protection
- Parent perceptions of stakeholder responsibility

Data Quality Procedures

To ensure data quality, multiple procedures were implemented, including:

- Geolocation check
- Bot detection: Captcha, OE analysis, PageTime variables
- Quota balancing on incoming sample demographics
- Positional straightliner check on MaxDiff exercise
- Digital fingerprinting
- Speeding checks
- Open-end quality review
- Duplicate detection
- Logic validation

Key Analytic Methodologies

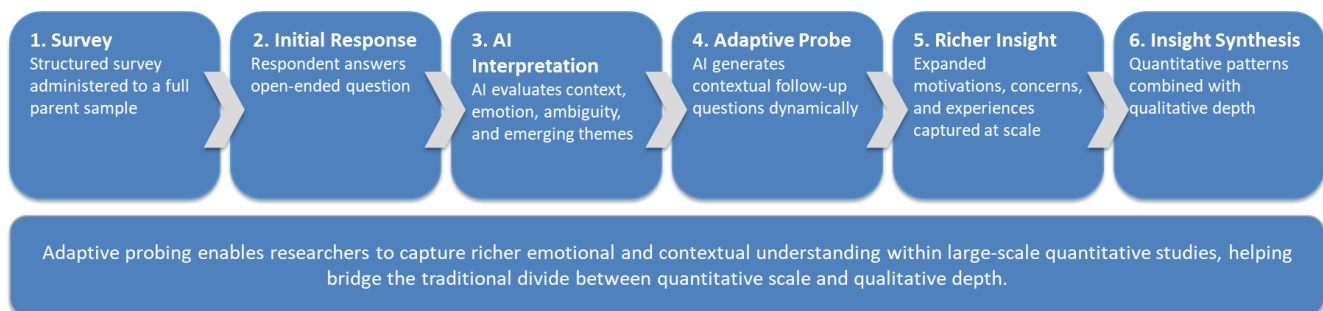
A core component of this project involved the use of advanced quantitative and AI-enabled methodologies to generate deeper behavioral understanding and actionable insights. Additionally, statistical significance testing was conducted at the 95% confidence level ($p < .05$), and statistically significant differences are referenced throughout the paper.

Generative AI-Powered Adaptive Probing

To better understand the contextual, emotional, and behavioral dynamics surrounding children’s online safety, the survey incorporated AI-powered adaptive probing techniques. Rather than relying solely on static open-ended responses, AI-generated follow-up questions were dynamically tailored to individual participant responses in real time. This approach allowed the survey to expand on short attitudinal statements and uncover richer insight related to parent concerns, trust dynamics, communication approaches, practical implementation challenges, and perceptions of online risk.

This approach enabled greater depth of qualitative understanding at scale, clarification of ambiguous responses, exploration of emotional nuance, identification of underlying motivations and barriers, and improved richness of open-ended data.

Figure 1: AI-Powered Adaptive Probing Process



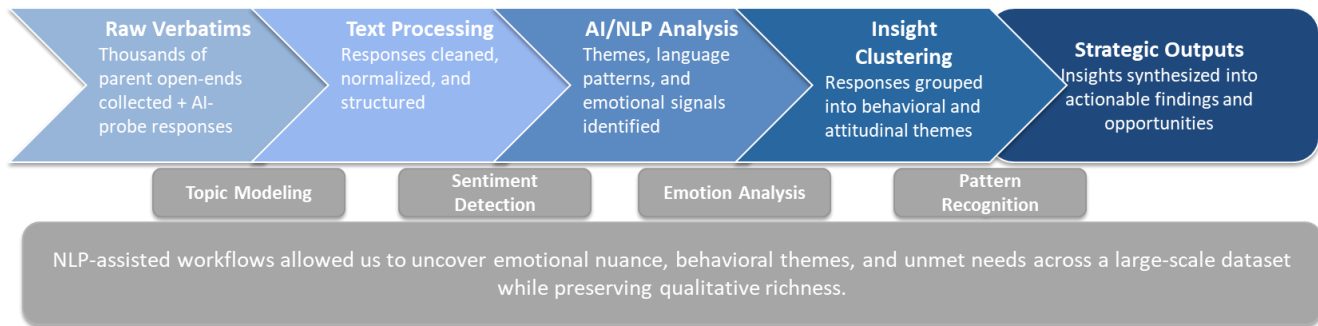
Across the sample, adaptive probing illustrated how AI-enabled probing may help bridge the gap between quantitative scale and qualitative depth within survey research by generating richer contextual understanding while maintaining the efficiency and scalability of large-sample quantitative methodologies. See Appendix E for more information on AI-enabled probing flows.

NLP-Assisted Verbatim Analysis

Natural language processing (NLP) approaches were used to support analysis of open-ended responses. Analysis dimensions included theme extraction, topic clustering, emotional tone analysis, sentiment analysis, risk-related language patterns, and parent anxiety and confidence indicators.

This process helped identify recurring themes across thousands of open-ended responses more efficiently and deeply than could have been done using manual coding. See Appendix F for more information.

Figure 2: NLP Assisted Verbatim Analysis Process



Latent Class Segmentation Modeling

Latent class segmentation analysis was conducted to identify distinct parent mindsets, behaviors, and approaches related to children's online safety management. See Appendix B for more details on the segmentation methodology. Rather than segmenting parents based on demographics or overall concern levels, the model incorporated attitudinal, behavioral, communication, technology-confidence, and decision-priority variables to identify naturally occurring parent profiles with differing approaches to online safety, monitoring, trust, intervention, and risk management.

The final segmentation solution was selected based on a combination of statistical fit, interpretability, segment stability, and practical differentiation across key online safety dimensions. Variables included in the model represented several core thematic areas, including:

- technical confidence and safety tool usage,
- online safety mindset and risk orientation,
- parent-child communication and trust dynamics,
- perceived and experienced online exploitation risks,
- and decision priorities when evaluating children's online activities and platforms.

The resulting segments revealed meaningful differences in how parents define preparedness, balance protection with independence, implement monitoring strategies, communicate with children, and evaluate online risks and safety solutions.

MaxDiff Prioritization Modeling

MaxDiff (Maximum Difference Scaling) analysis was conducted to identify the relative importance of online safety solutions, features, and intervention approaches from the parent perspective. See Appendix C for more details on this methodology. Respondents were shown sets of potential online safety solutions and asked to identify the most and least important options within each set. This approach forced respondents to make trade-offs between competing priorities, helping reduce scale bias and providing stronger differentiation than standard rating scales.

The MaxDiff exercise included a range of online safety solutions, and the final list of solutions included in the MaxDiff exercise was particularly challenging for this research given the sensitivity and importance of

the topic. Initially, the exercise was planned with a large set of individual features, however at that level, trade-offs proved too difficult for respondents (e.g., identifying adults posing as children vs recognizing grooming behaviors vs recognizing explicit images). Success was achieved by grouping sets of features into differentiated solution categories.

Hierarchical Bayes estimation was used to generate individual-level utility scores, which were then normalized to support relative importance comparisons across solutions. The analysis was designed not only to identify the highest-priority solutions overall, but also to better understand the underlying philosophies parents apply when evaluating online safety interventions.

To further explore differing parent solution preferences, cluster analysis was conducted using respondent-level MaxDiff utility scores. This analysis identified distinct groups of parents with differing approaches to online safety management, intervention priorities, and technology preferences.

Multiple cluster solutions were evaluated based on statistical separation, interpretability, stability, and practical differentiation across solution priorities. The final solution identified three distinct solution-orientation clusters.

The resulting framework provided a more nuanced understanding of how parents evaluate online safety solutions beyond overall importance scores alone, helping identify differing expectations regarding the role of parents, technology platforms, automation, and AI-enabled systems in protecting children online.

Driver Analysis by Segment

To better understand what most strongly influences parents' sense of preparedness to manage online safety risks, driver analysis was conducted using Johnson's Relative Weights methodology. The dependent variable measured perceived preparedness to prevent or respond to serious online safety risks, while independent variables included online safety mindset, technical confidence, use of safety tools, technology experience, and communication approach.

The strength of this method was especially apparent when assessing the drivers by segment, which resulted in identifying key levers to build parent confidence within each of the parent segments. See Appendix D for more details on the driver analysis.

AI-Enabled Intervention Development

Moving Beyond Insight Generation

A distinguishing aspect of this project was the intentional focus on translating research insights into actionable intervention frameworks.

Market research initiatives often end with reporting findings and recommendations. However, organizations frequently struggle to turn insights into practical tools, communication strategies, educational approaches, or behavioral interventions.

This project explored how AI-enabled systems can help accelerate the progression from insight generation toward intervention development and implementation strategies - a roadmap for success including near-term and longer-term actions for stakeholders.

Use of the Amplifyer Platform

Amplifyer's proprietary AI platform was used as a multi-agent strategic intelligence, insight synthesis, concept-development, communication planning and strategic analysis system.

The AI platform was used to:

- Simulate stakeholder and subject-matter-expert ideator perspectives
- Accelerate strategic ideation, using codified design-thinking methodologies
- Produce novel, disruptive solutions with impact assessments
- Generate communication concepts targeted to stakeholders
- Develop supporting parental frameworks
- Create intervention roadmaps

The platform was not used to replace researchers or automate conclusions. Amplifyer is a Human-at-the-Helm platform deploying agents under the direction of researchers, designed to augment intelligence and accelerate discernment by subject matter experts. It serves as a collaborative acceleration system to help researchers and organizations more rapidly operationalize findings. Amplifyer was designed to increase human agency by accessing a wide swath of intelligence, processing vast arrays of insights, performing extensive time-consuming strategic analysis using codified frameworks and best practices, conducting a rigorous design-thinking process to develop solution prototypes, simulate insights based on these prototype concepts, and finally spinning up a virtual marketing team to develop marketing, PR, branding and communication strategies.

Implications of AI-Enabled Insight Operationalization

The use of AI-enabled strategic platforms may represent an important evolution in market research.

Implications for Research Practice

One of the more significant implications of this study extends beyond the substantive findings themselves and into how research can be conducted and applied. The project demonstrated how AI-enabled

methodologies can support multiple stages of the research lifecycle, from research design through insight generation to concept development and implementation. Rather than functioning solely as tools for analysis, AI-enabled systems may increasingly help researchers:

- Generate and refine research hypotheses
- Explore alternative questionnaire structures and probing approaches
- Accelerate analysis and synthesis of complex datasets
- Gather and interpret related data that resides outside of the dataset
- Identify patterns, tensions, and opportunities across multiple data sources
- Develop strategic frameworks that connect findings to decision-making
- Create tailored storytelling and communication approaches for different stakeholder audiences
- Support futurecasting and scenario planning exercises

Importantly, the findings suggest that AI is most valuable when used to augment researcher expertise. Human judgment remained essential throughout the project for methodology design, interpretation, validation, and prioritization of insights.

Implications for Organizations and Stakeholders

The study also illustrates how AI-enabled insight operationalization may help organizations migrate more effectively from understanding problems to implementing solutions. Frequently, research projects conclude with findings and recommendations, while organizations and stakeholders are then responsible for determining how best to translate those insights into practical tools, communication strategies, educational approaches, or interventions. In this project, AI-enabled strategic modeling tools were used to explore an array of potential interventions, communication approaches, educational resources, and implementation pathways directly informed by the research findings.

Potential applications include:

- Creating intervention roadmaps tailored to specific parent segments
- Identifying opportunities for new products, services, or safety features
- Developing targeted parent education and awareness initiatives
- Building communication strategies designed for specific stakeholder groups
- Facilitating stakeholder alignment around complex societal challenges
- Supporting long-term planning through scenario development and future-oriented analysis

The ability to efficiently tailor recommendations, communications, and intervention approaches to the needs, priorities, and characteristics of different audiences may be particularly valuable for complex issues such as child online safety, where effective solutions often require coordinated engagement across children, parents, educators, policymakers, technology providers, and child-protection organizations simultaneously.

Key Findings

Key Takeaways: Overall Findings & the Online Safety “Protection Gap”

The findings reveal a digital environment in which children are engaging across a wide range of platforms, devices, and online ecosystems at increasingly early ages, while many parents are still navigating how to effectively manage online safety risks. Although most parents recognize meaningful online threats and report taking at least some protective actions, the research consistently identified a “protection gap” between awareness of risk, confidence in protection, and consistent, effective implementation of safety practices and tools.

Children Are Embedded in Complex Digital Ecosystems

Children’s online activity spans smartphones, gaming platforms, messaging applications, social media, AI tools, streaming environments, and anonymous interaction platforms. The most commonly used devices include smartphones (75%), gaming devices (74%), smart TVs/streaming devices (74%), and tablets (64%).

Importantly, children begin using many connected devices at relatively young ages. Tablets are often introduced before age 8 (and 3/10 at age 5 or earlier), while smartphones and wearables increasingly appear during late elementary and middle school years. This creates an environment where parents are expected to manage multiple devices, multiple platforms, evolving risks, and highly dynamic digital behaviors simultaneously.

Parents Recognize Significant Online Risks

Online safety concerns are widespread:

- one-third of parents perceive their children as facing high or very high levels of online risk exposure,
- while nearly half perceive at least moderate levels of risk.

Parents consistently expressed concern about online predators and grooming, inappropriate or explicit content, scams and phishing, cyberbullying, harmful communities, excessive usage, misleading information, and stranger interactions.

Risk perceptions extended across social media, messaging apps, gaming ecosystems, anonymous chat applications, AI-powered tools, and betting/prediction platforms. Notably, platforms involving anonymous interaction, open communication, stranger access, or relationship-based interactions were frequently perceived as especially risky.

Most Parents Are Trying — But Many Struggle

The findings show that most parents are actively attempting to manage online safety: nearly all use at least some type of safety tool, most report implementing rules or controls, and many engage in regular conversations with children about online behavior.

Common actions include discussing online safety, requiring approval for app downloads, monitoring app or browsing activity, using parental controls, setting screen-time rules, and restricting certain features or platforms. At the same time, about one-third regularly monitor activity, about one-third use parental control software, and 1 in 10 parents report taking no specific actions at all.

This suggests that awareness of risk does not always translate into sustained protective behavior.

The Protection Gap Emerges Across Multiple Dimensions

One of the strongest themes across the findings is the existence of a “protection gap” between concern and practical implementation. This gap appears in several forms.

1. Risk Awareness vs. Action

Although most parents acknowledge meaningful online risks, many rely primarily on conversations rather than layered protection strategies, and relatively few consistently use advanced monitoring or filtering tools.

2. Confidence vs. Practical Capability

While 72% say they can independently set up parental controls, about one-quarter still require help, and roughly one-third report only basic technical capability or reliance on others for technology support.

Parents commonly turn to online searches, YouTube tutorials, spouses, and even their own children for technology help. This highlights a practical implementation challenge: many parents may conceptually support online safety measures but lack the confidence, time, or technical fluency to consistently action them.

3. Desire for Monitoring vs. Privacy Concerns

The single largest challenge parents identified is balancing children’s privacy with monitoring. Additional barriers include children resisting controls, uncertainty about which risks matter most, lack of effective tools, time constraints, and disagreement among caregivers. This suggests many parents are struggling not only with what tools to use, but also with how much oversight is appropriate.

4. Communication Confidence vs. Actual Communication Dynamics

While 76% believe their children would probably or definitely come to them with online concerns, the broader communication findings suggest a more nuanced reality. Only about one-third report setting clear rules, many primarily step in only when issues arise, and roughly 1 in 10 do not typically initiate online safety conversations.

This indicates that some parents may overestimate communication openness, visibility into children’s experiences, or children’s willingness to disclose concerning events.

Parents Want Balance — Not Total Surveillance

The findings suggest that most parents are not seeking unrestricted surveillance. Instead, many appear to be searching for balanced oversight, practical guidance, age-appropriate controls, and tools that preserve trust and independence while still reducing risk.

This tension appears repeatedly throughout the findings: parents want visibility, but also want to maintain trust, autonomy, and healthy family dynamics.

AI and Emerging Platforms Add New Complexity

The research also highlights the growing complexity introduced by AI-powered tools, anonymous communication apps, algorithm-driven content systems, and rapidly evolving digital ecosystems. Many parents are still unfamiliar with newer platforms and AI tools, yet several of these environments were perceived as carrying moderate-to-high levels of risk. This suggests a widening challenge where children's digital behaviors may evolve faster than parent awareness and preparedness.

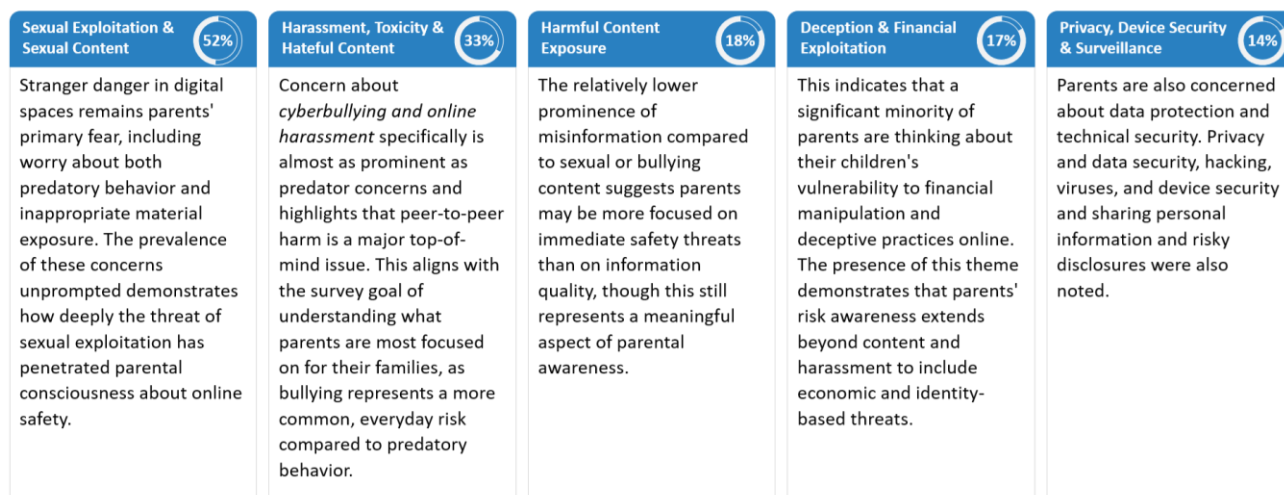
Strategic Implications

Taken together, the findings suggest that effective online safety strategies must go beyond simply increasing awareness. Parents may need:

- simpler and easier-to-use tools,
- clearer prioritization guidance,
- more actionable support,
- stronger communication frameworks,
- and adaptive systems that help translate concern into meaningful protective action.

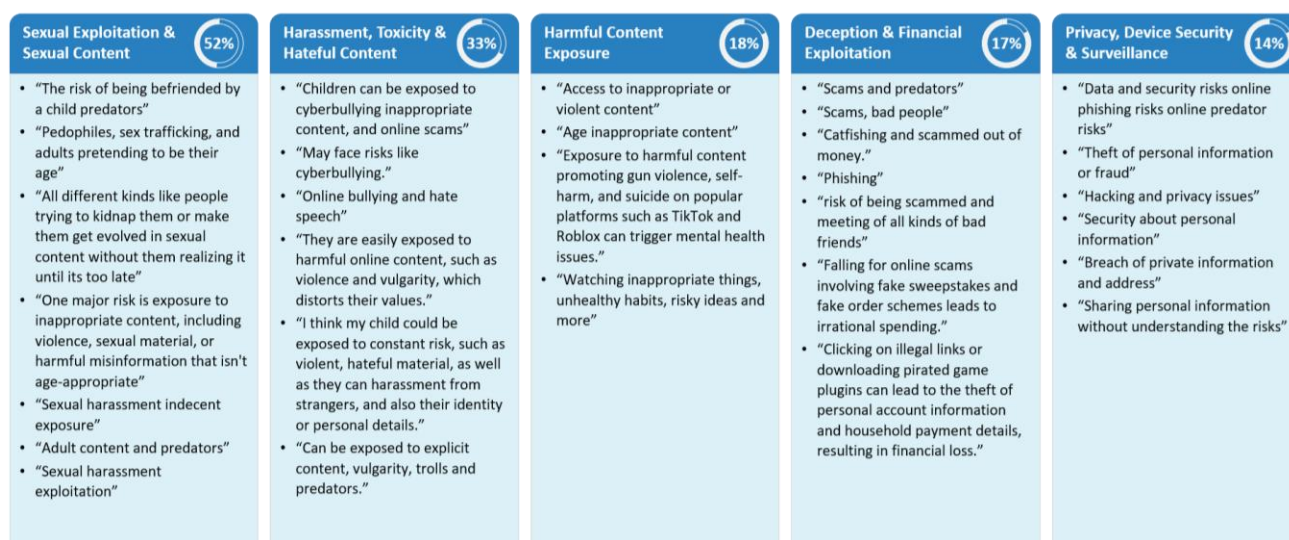
The findings also suggest that online safety is no longer simply a technology problem. It is increasingly a communication challenge, a behavioral challenge, a trust challenge, and a digital parenting challenge requiring coordinated support across families, platforms, educators, policymakers, and technology providers.

Figure 3: Types of Children's Risk Exposure



Base: Total - 1014
T7. What type of risks do you think your child(ren) could be exposed to when online?

Figure 4: Verbatim Responses Related to Types of Children's Risk Exposure

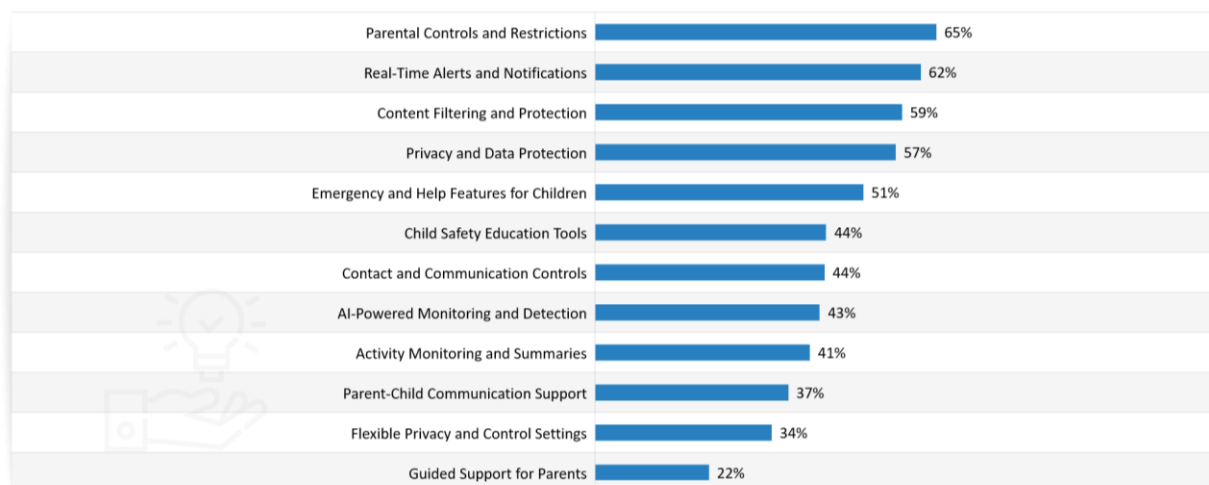


Base: Total - 1014
T7. What type of risks do you think your child(ren) could be exposed to when online?

Solution Prioritization & MaxDiff Cluster Analysis

The MaxDiff analysis revealed that parents strongly prioritize online safety solutions that provide direct protection, monitoring, and intervention capabilities. While parents expressed interest in a broad range of online safety approaches, the strongest demand consistently centered on solutions that actively help parents manage or reduce online risk exposure.

Figure 5: Prioritization of Solutions – Probability of Choice



Base: Total – 2014
V1. When it comes to solutions to help keep your child(ren) safe online... Which are you MOST INTERESTED in?... Which are you LEAST INTERESTED in?

Core Solution Priorities

The highest-priority solutions across parents are Parental Controls and Restrictions, Real-Time Alerts and Notifications, Content Filtering and Protection, and Privacy and Data Protection. These findings suggest that parents are primarily seeking visibility, control, active intervention, and automated protection mechanisms rather than passive or informational support alone.

Solutions that rank substantially lower overall are focused primarily on communication support, parent guidance, and educational tools.

Protection-Oriented Solutions Dominate

The strongest-performing solutions all center around the theme of active protection. Parents show the greatest interest in tools that block harmful content, monitor activity, identify risks, limit unsafe interactions, or notify parents when concerns arise.

This indicates that many parents view online safety primarily as a risk-management and intervention challenge, rather than solely an educational or communication issue.

Opportunity Gaps in the Market

The analysis identified several important gaps between:

- perceived importance,
- perceived effectiveness,
- and current usage.

Most notably, Real-Time Alerts and Notifications and Emergency and Help Features for Children have high interest levels, but current usage rates are substantially lower. This suggests meaningful unmet demand for proactive warning systems, escalation support, and child-accessible emergency tools.

Similarly, only 39% currently use parental controls, 32% use content filtering, and 31% use privacy/data protection tools while 14% report using none of the assessed solutions at all.

These findings reinforce the existence of a broader protection implementation gap between parent concern and actual protective behavior.

Communication and Education Solutions Face Credibility Challenges

Several of the solutions with the lowest credibility focused on communication support, parent guidance, and educational approaches. Specifically, Parent-Child Communication Support, Guided Support for Parents, and Child Safety Education Tools were among the least likely to be viewed as highly effective. This does not necessarily mean parents oppose these solutions. Rather, it suggests many parents may perceive educational approaches alone as insufficient relative to the scale and complexity of online risks.

AI-Based Protection Has Meaningful Consumer Acceptance

One of the more notable findings is that AI-powered monitoring and detection performed substantially better than many softer communication-based solutions. Parents appear increasingly open to AI-enabled systems that proactively identify threats, detect concerning patterns, and surface actionable alerts. This is particularly important given the increasing scale, speed, and complexity of children's digital environments, where manual parent oversight alone may not feel sufficient.

Child Age Has Limited Impact on Priorities

Importantly, solution priorities are remarkably consistent across age groups, with similar prioritization patterns across both decision factors and preferred safety solutions. This suggests that concerns about online safety, demand for intervention tools, and desire for protection extend consistently across a wide child age range.

Solutions Cluster into Three Distinct Solution Mindsets

Latent class analysis of the MaxDiff results revealed three distinct solution-orientation clusters:

1. Hands-On Control (23%)

This group favors direct, parent-led management approaches, suggesting parents should remain highly involved in controlling and managing their child's online environment. This cluster showed extremely high prioritization of parental controls, alerts, filtering, and communication restrictions, while showing almost no interest in AI-powered monitoring or parent-child communication support.

2. Balanced Safety (53%)

The largest cluster favors a more moderate, balanced, and practical approach that suggests online safety is important, but solutions should support healthy family dynamics and avoid becoming overly intrusive: protection, communication, education, and family usability.

Unlike the other clusters, this group does not have extremely polarized preferences. Instead, they showed moderate interest across a broad range of solutions. Importantly, they were the only cluster to rank Child Safety Education Tools (#1) and Parent-Child Communication Support (#2) as top priorities.

This indicates many parents still value communication and education but prefer these approaches when positioned as part of a balanced safety ecosystem rather than as standalone interventions.

3. Automated Protection (24%)

This group shows extremely high interest in AI-powered monitoring, real-time alerts, automated content filtering, and detection-based approaches while placing very low value on communication-oriented solutions. This leads to the idea that technology itself should play an active role in identifying and preventing online risks.

Figure 6: Probabilities of Choice

CLUSTER 1 Hands-On Control 23%		CLUSTER 2 Balanced Safety 53%		CLUSTER 3 Automated Protection 24%	
Parental Controls and Restrictions - Lets parents block apps, limit access, and control what their child can do online	89%	Child Safety Education Tools - Teaches children how to recognize risks and make safer decisions online	64%	Real-Time Alerts and Notifications - Immediately alerts parents when concerning behavior or interactions are detected	89%
Privacy and Data Protection - Prevents sharing of personal information and ensures the child's data is kept secure and private	77%	Parent-Child Communication Support - Provides tools and prompts to help parents talk with their children about online safety	58%	Content Filtering and Protection - Blocks or filters inappropriate, explicit, or harmful content automatically	88%
Contact and Communication Controls - Limits who children can interact with and blocks unknown or suspicious contacts	64%	Guided Support for Parents - Gives parents clear recommendations and guidance on what to do when issues arise	37%	AI-Powered Monitoring and Detection - Automatically scans messages and activity to detect risks like bullying, grooming, or inappropriate content	86%
Emergency and Help Features for Children - Includes SOS buttons and easy ways for children to report concerns or ask for help	58%	Flexible Privacy and Control Settings - Lets families choose the balance between monitoring and child privacy based on age or preference	37%	Activity Monitoring and Summaries - Provides clear summaries of apps used, contacts, and overall online activity	44%
PROBABILITIES OF CHOICE					

Base: Total - 1014, Hands-on Control - 232, Balanced Safety - 539, Automated Protection - 243

Strategic Implications

The MaxDiff findings suggest several important implications for organizations developing online safety products and interventions:

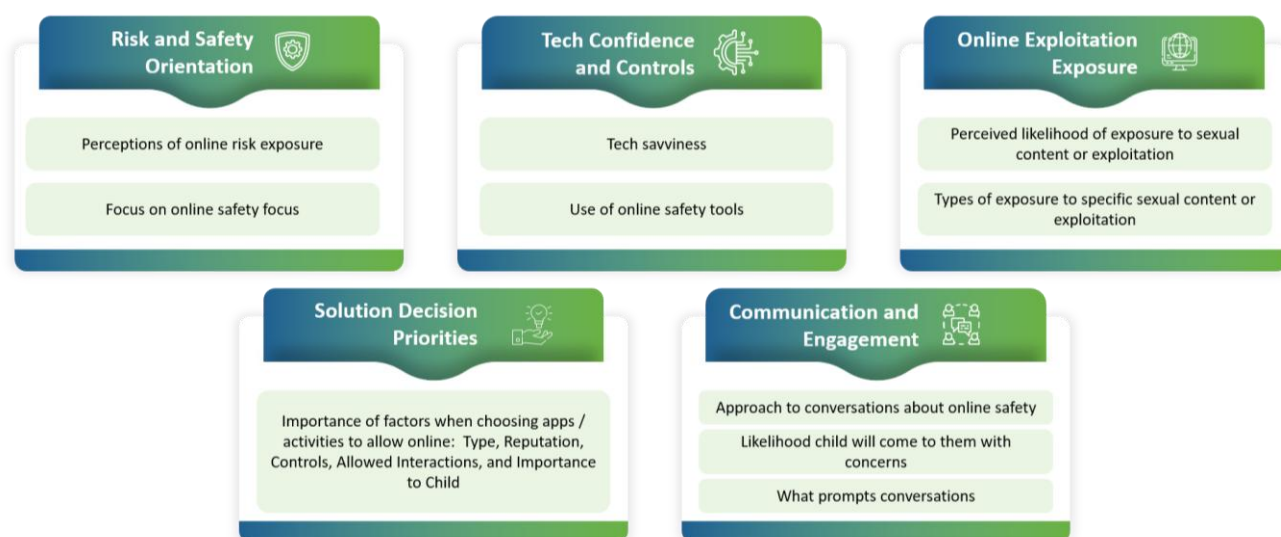
- Parents strongly prefer actionable protection tools over passive guidance alone
- Solutions that combine automation with parent visibility may have particularly strong market potential
- Communication and education are important, but may need to be integrated into broader protection ecosystems rather than positioned independently

- There is substantial opportunity to close the implementation gap between perceived importance and actual solution usage
- AI-enabled monitoring and detection systems appear increasingly acceptable to many parents when framed around protection, alerts, and risk prevention rather than surveillance alone

Segmentation: Distinct Parent Segments Require Different Solutions

The latent class segmentation revealed that parents approach children's online safety through distinctly different mindsets, behaviors, and management styles rather than through simple differences in overall concern levels. Five core dimensions drove segmentation classification:

Figure 7: Segmentation Dimensions



Four Distinct Parent Segments Emerged

Pragmatic Balancers (41%)

The largest segment takes a moderate and practical approach to online safety, balancing protection with allowing children normal online experiences. They are less technically confident, less proactive, and less likely to use advanced monitoring tools than other segments. They are also more likely to trust their children to manage themselves and to only step in when issues arise.

Vigilant Managers (12%)

This segment is highly proactive, technically sophisticated, and deeply focused on monitoring and control. They actively use and customize multiple safety tools and place particularly high importance on parental controls and monitoring capabilities when evaluating solutions.

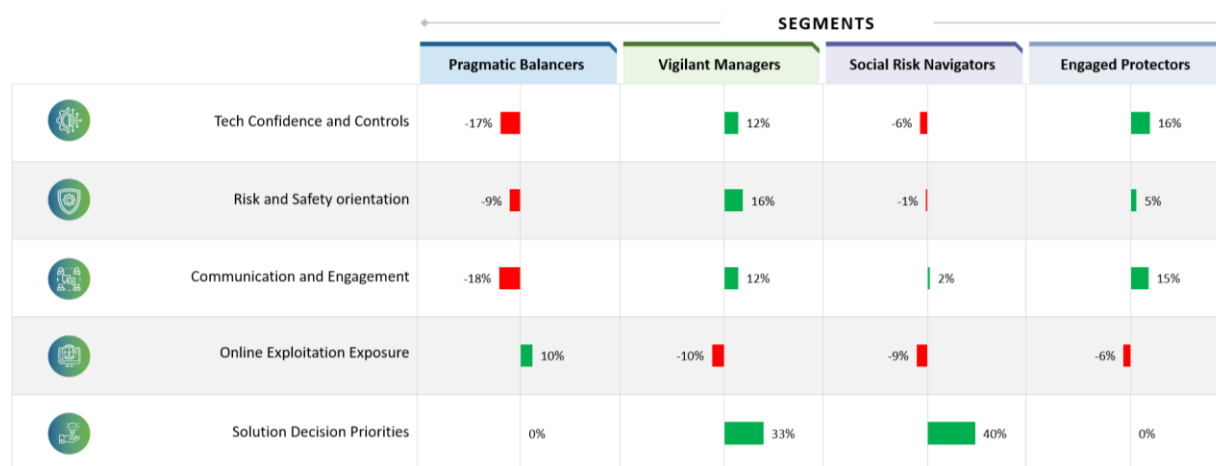
Social Risk Navigators (11%)

These parents are especially focused on who their children interact with online and view online safety primarily through the lens of interpersonal and interaction-based risks. They tend to rely on selective intervention rather than intensive ongoing monitoring.

Engaged Protectors (37%)

This segment combines high technical confidence with strong communication and ongoing engagement with children. Compared with other segments, they are most likely to foster open conversations, maintain regular communication about online safety, and actively implement a broad range of safety actions and tools.

Figure 8: Segmentation Dimensions: Variance From Average



Key Cross-Segment Insights

1. Online Safety Is Not a One-Size-Fits-All Problem

Parents differ substantially in how they perceive online risks, how actively they intervene, how much they trust their children, how often they communicate, and what types of solutions they value most.

Online safety education, tools, and interventions will likely be more effective when tailored to different parent mindsets and management approaches rather than relying on universal messaging.

2. Technical Confidence Strongly Influences Safety Management

Engaged Protectors and Vigilant Managers report the highest levels of technology confidence and are also the most likely to customize safety tools, monitor online activity, implement parental controls, and take proactive safety actions.

In contrast, Pragmatic Balancers are significantly more likely to rely on others for technology support, avoid advanced tools, and use only basic controls or no tools at all.

This highlights a meaningful capability gap that may limit some parents' ability to translate concern into action.

The Protection Gap

One of the clearest findings across the segmentation is the existence of the “protection gap”. Specifically, many parents acknowledge meaningful online risks, but their behaviors, monitoring practices, communication patterns, and solution usage do not always align with the level of exposure they believe children face.

Several findings support this gap:

- Pragmatic Balancers are among the least proactive segments despite reporting comparable perceptions of online risk exposure to other groups.
- Only 57% of Pragmatic Balancers believe their children would probably or definitely come to them with concerning online experiences, compared with over 90% among Engaged Protectors and Vigilant Managers.
- Pragmatic Balancers are also the least likely to use parental control tools, monitor usage, or regularly discuss online safety topics with their children.
- Despite lower levels of monitoring and intervention, Pragmatic Balancers are among the most likely to report that their children had experienced inappropriate or exploitative online interactions.
- Across segments, many parents identified practical barriers including balancing privacy with monitoring, children resisting controls, lack of time, and uncertainty about what risks to prioritize.

Taken together, these findings suggest that awareness of online risks alone is insufficient. Parents may require simpler and more usable tools, clearer guidance, better communication frameworks, and more actionable support systems to effectively translate concern into protective action.

Communication and Trust Matter

The segmentation also demonstrates that communication dynamics may play a critical role in online safety outcomes.

Engaged Protectors and Vigilant Managers are substantially more likely to report regular conversations about online safety, children bringing concerns directly to them, and broad discussion of online risks and behaviors.

In contrast, Pragmatic Balancers and Social Risk Navigators are more likely to communicate only occasionally, wait until issues arise, or rely more heavily on children to self-manage online behavior.

This indicates that parent-child communication quality and consistency may be an important component of effective online safety management.

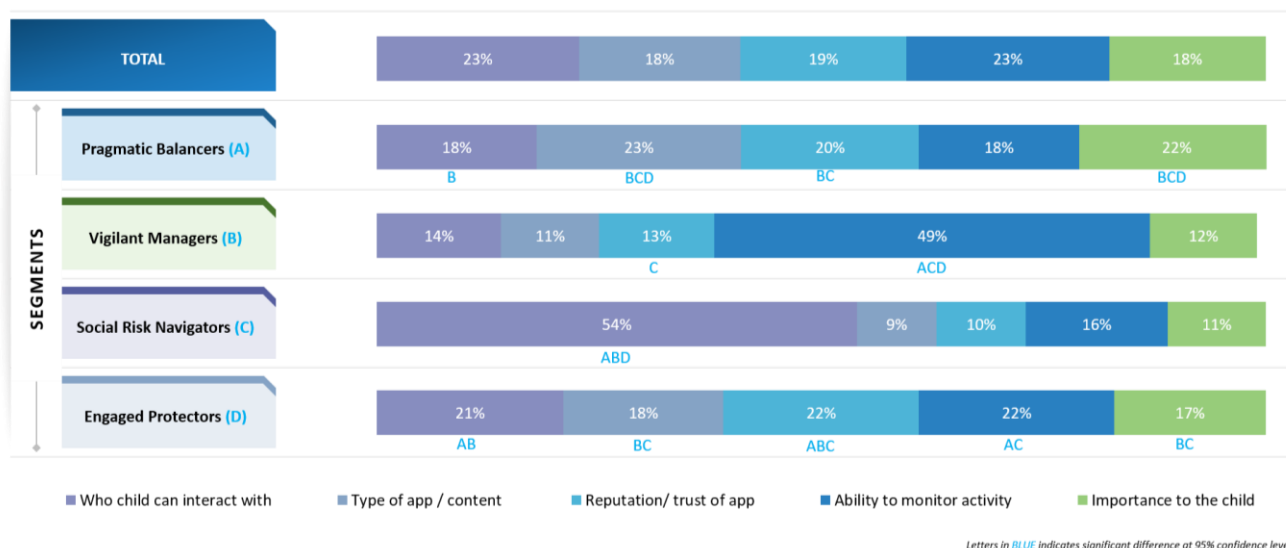
Parent Segments Prioritize Different Types of Solutions

The segmentation revealed substantial differences in what parents value most in online safety solutions:

- Vigilant Managers strongly prioritize monitoring and control capabilities.
- Social Risk Navigators prioritize who children can interact with online.
- Pragmatic Balancers gravitate toward “Balanced Safety” solutions rather than highly restrictive or heavily automated approaches.
- Engaged Protectors show broad interest across multiple solution types and report the highest current usage of online safety tools.

These findings reinforce the need for differentiated approaches to product design, messaging, and educational support.

Figure 9: Decision Factors for Solutions



Strategic Implications from Segmentation

The findings suggest several important implications for organizations working in child online safety:

- Online safety solutions should accommodate different parenting philosophies and technical confidence levels.
- Simplification and usability may be critical for increasing adoption among less technically engaged parents.
- Communication-based interventions may be as important as monitoring technologies alone.
- Parents may benefit from more practical guidance on prioritizing risks and translating awareness into effective action.
- AI-enabled systems may help personalize recommendations, communication frameworks, and intervention pathways based on different parent profiles and needs.

Driver analysis further supports the need for different strategies

Driver analysis revealed that preparedness is not driven uniformly across parents. Instead, different parent segments rely on different combinations of technical capability, risk orientation, communication style, and online safety behaviors when evaluating their own readiness to protect children online.

Across the full sample, the strongest driver of preparedness is the perceived capability to independently set up and manage online safety controls (49% of explained variance), followed by: online safety mindset and risk orientation (24%), current use of safety tools (14%), technology experience (9%), and communication approach (4%).

These findings suggest that parents' sense of preparedness is driven primarily by confidence in their ability to implement protections, rather than by communication behaviors alone.

Pragmatic Balancers

Among Pragmatic Balancers, preparedness is overwhelmingly driven by technical capability (62%), followed by: safety mindset and risk orientation (29%).

Current tool usage, technology experience, and communication behaviors played only minor roles. Many parents in this segment may conceptually value online safety but lack confidence in their ability to effectively implement protections. The findings reinforce the broader “protection gap” identified throughout the study, where awareness of online risks does not necessarily translate into operational confidence or sustained protective action.

Vigilant Managers

Vigilant Managers differ notably from the other segments. For this group, preparedness is driven more heavily by online safety mindset and risk orientation (41%) than by technical capability (24%).

This segment already reported high levels of proactive behavior, monitoring, and safety tool usage throughout the study. As a result, their preparedness appears to stem less from learning how to implement protections and more from maintaining a strong protective mindset and ongoing vigilance regarding online risks.

Communication behaviors also play a larger role for this segment than for most others (15%), suggesting that active discussion and engagement may reinforce their broader protection-oriented parenting approach.

Social Risk Navigators

Among Social Risk Navigators, preparedness is shaped by a more balanced combination of technical capability (40%), safety tool usage (24%), and technology experience (26%).

Unlike the other segments, this group places comparatively greater emphasis on overall technology familiarity and experience. This finding aligns with broader segmentation results showing that these parents are particularly focused on interpersonal and interaction-based online risks rather than solely on broad monitoring or control strategies.

Their preparedness appears to depend less on intensive oversight and more on having sufficient digital familiarity and practical experience to navigate social and interaction-related risks as they arise.

Engaged Protectors

For Engaged Protectors, preparedness is also driven primarily by technical capability (66%), although this segment already reported relatively high levels of existing engagement, communication, and safety tool usage. Current tool use contributed meaningfully to preparedness perceptions (18%), while communication behaviors contributed very little independently.

This suggests that among highly engaged parents, preparedness is less about awareness or conversations alone and more about confidence in maintaining layered, practical safety systems.

Key Implications

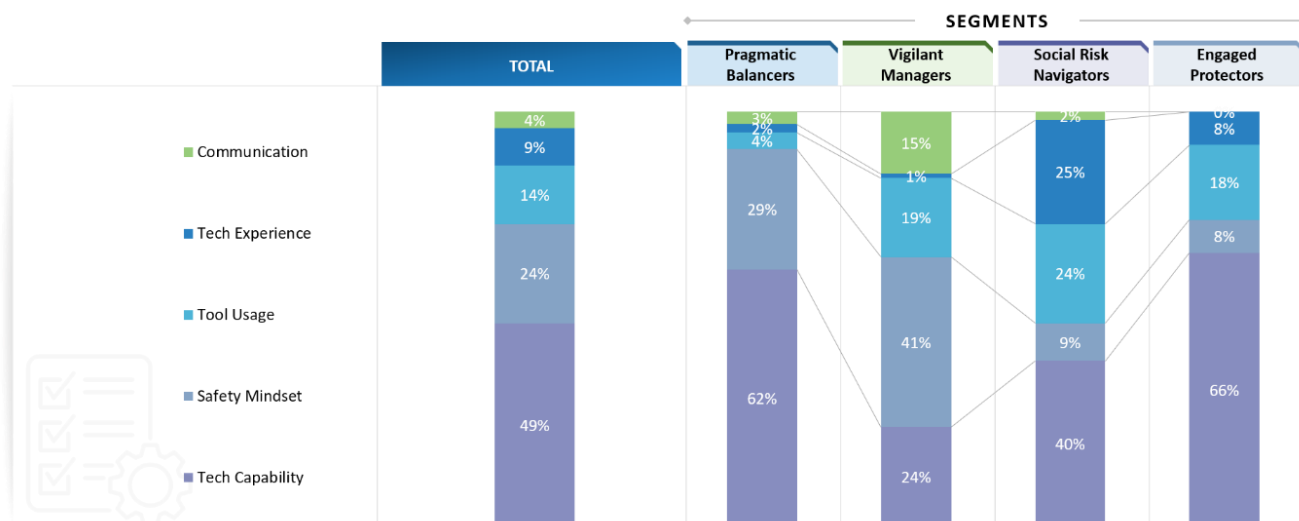
Overall, the driver analysis reinforces that the online safety “protection gap” is not simply a matter of awareness. Most parents already recognize that meaningful online risks exist. Instead, preparedness appears to depend heavily on confidence, practical implementation capability, and parents’ ability to translate concern into sustained protective action.

The findings also suggest that online safety interventions may need to be tailored differently by parent segment:

- some parents may benefit most from simplified tools and implementation guidance,
- others may require support around communication and trust-building,
- while highly proactive parents may respond more strongly to advanced monitoring, automation, and risk-detection capabilities.

These findings further reinforce the importance of designing online safety ecosystems that accommodate differing parenting styles, technical confidence levels, and approaches to balancing protection with independence.

Figure 10: Drivers of Preparedness



AI-Enabled Intervention Outputs

Plausible Future Scenarios

As part of the AI-assisted strategic synthesis process, Amplifyer generated futurecasting scenarios to explore how child online safety ecosystems may evolve over the next decade under differing combinations of technological maturity, regulatory environments, privacy expectations, and platform governance models.

The scenarios highlighted growing tension between increasing demands for privacy and encryption, decentralized and federated online environments, rapid expansion of generative AI capabilities, and escalating pressure for stronger online child protection mechanisms.

Across the futurecasting exercise, one of the most consistent themes was the potential widening of the “protection gap” as digital ecosystems become more fragmented, encrypted, AI-driven, and difficult for parents, platforms, and regulators to monitor using traditional approaches.

Several major trends emerged as particularly important:

- the expansion of end-to-end encrypted communications,
- the shift toward decentralized social and digital platforms,
- increasing use of privacy-preserving cryptographic identity systems,
- and the rapid growth of synthetic AI-generated exploitation content.

The futurecasting exercise generated four plausible future-state scenarios representing different combinations of technology maturity and governance approaches. See Appendix G for more details.

The Dark Fracture

This scenario envisioned a highly fragmented digital ecosystem shaped by punitive regulation, failed standardization efforts, and breakdowns in collaborative governance. In this future, decentralized and encrypted platforms become difficult to monitor effectively, safety systems remain inconsistent, and children face elevated exposure to exploitation risks due to limited coordination and weak moderation infrastructure.

The Cryptographic Panopticon

This scenario described a future dominated by highly standardized, technically rigorous compliance systems in which cryptographic verification, edge-based monitoring, and tightly regulated privacy frameworks become the primary mechanisms for balancing online safety and encryption. While safety enforcement becomes highly effective, the environment also introduces concerns around rigid governance, heavy compliance burdens, and reduced flexibility.

The Trust-by-Design Commons

This scenario represented the most collaborative and optimistic future state. In this environment, decentralized platforms, safety organizations, and technology providers work together through open

standards, privacy-preserving verification systems, and cooperative governance frameworks to create safer digital ecosystems without relying on invasive surveillance or centralized control.

The Vulnerable Archipelago

This scenario illustrated a future in which decentralized platforms continue to expand, but safety infrastructure and governance fail to mature at the same pace. Volunteer moderators, fragmented communities, and inconsistent tools struggle to manage rapidly evolving exploitation risks and AI-generated harmful content, leaving significant gaps in child protection systems.

Across scenarios, several strategic implications consistently emerged. The analysis suggested that future online safety ecosystems may increasingly require:

- privacy-preserving safety technologies,
- decentralized trust and verification systems,
- AI-enabled detection and moderation capabilities,
- collaborative governance frameworks,
- and tools that help parents balance protection with trust and autonomy.

The futurecasting exercise also reinforced one of the broader themes identified throughout the research: traditional approaches to online safety management may become increasingly insufficient as digital ecosystems evolve faster than existing safety frameworks, governance structures, and parent and child preparedness models.

Technical Guidance and Risk Mitigation Outputs

The Amplifyer platform was also used to generate exploratory technical guidance and implementation concepts related to online child safety systems. These outputs focused on how AI-enabled, privacy-preserving safety architectures may help address emerging online exploitation risks while balancing concerns related to privacy, autonomy, trust, and regulatory compliance.

A key Amplifyer output was the development of a risk assessment and mitigation matrix identifying potential implementation risks associated with AI-enabled child safety systems, along with potential mitigation approaches.

While these outputs represent exploratory concepts and narrative prototypes rather than validated production systems, they illustrate how AI-enabled strategic synthesis platforms may help extend research beyond insight generation into practical implementation planning, operational risk assessment, and solution-oriented framework development.

Table 1: Technical Guidance and Risk Mitigation Outputs

Risk Category	Identified Risk	Severity	Tactical Mitigation Strategy
Technological Evasion	Sophisticated predators may evade local NLP classifiers by using coded language, slang, or shifting entirely to non-text media.	Medium	Integrate a hybrid cascading system that pairs semantic NLP models with localized, on-device image hash matching (e.g., PhotoDNA) and behavioral anomaly triggers, such as sudden contact from unlinked, newly created accounts.
System Usability & Fatigue	Warning fatigue and system usability issues caused by false-positive triggers in everyday casual conversations.	Medium	Incorporate a localized social asymmetry index into the decision boundary equation. The system should suppress high-friction alerts in conversations between users with verified mutual connections, similar account ages, or existing contact histories.
Hardware Limitations	Thermal throttling and severe battery drain on low-spec mobile devices running continuous transformer-based models.	High	Implement a tiered execution framework. Lightweight regular expressions and keyword scanners run continuously, waking the heavier NLP transformer only when a baseline risk threshold is crossed. This limits high-power processing to active threat scenarios.
User Backlash & Privacy Concerns	Privacy advocates or users may push back, viewing on-device scanning as a form of client-side surveillance or a threat to encryption.	High	Maintain clear data separation. Ensure no raw text, media, or classification metadata ever leaves the physical device without explicit user action or report submission. This design should be validated through independent, third-party cryptographic audits.

AI-Enabled Concept Development Using DesignThinker

To extend the study beyond descriptive segmentation and into practical intervention development, the Amplifyer DesignThinker platform was used to generate tailored digital safety concepts for each of the four parent segments identified in the research. Rather than producing generalized recommendations, the system synthesized segmentation findings, behavioral patterns, emotional tensions, platform usage, online risk exposure, and parental decision-making dynamics into segment-specific solution ecosystems. DesignThinker facilitated a simulated workshop of over a dozen qualified experts to develop compelling solutions.

Across all four segments, the AI-enabled ideation process consistently identified a central challenge in today's digital parenting: balancing child safety with trust, autonomy, privacy, and healthy family relationships. While each segment approached this challenge differently, the outputs demonstrated how highly differentiated solution architectures may be required to address the distinct emotional and behavioral realities of families.

Pragmatic Balancers

For Pragmatic Balancers (41% of parents), the DesignThinker process focused on the tension between maintaining trust and providing sufficient oversight. This segment tended to avoid highly invasive monitoring despite experiencing meaningful exposure to online safety risks. The generated concepts emphasized “balanced safety” approaches that reduced technical complexity while preserving family autonomy and communication.

Three primary concepts emerged:

- **TrustProxy Privacy Anomaly Engine** — a privacy-preserving behavioral risk detection platform using on-device processing and contextual risk alerts without exposing raw communications.
- **CalmResponse Emergency Protocol** — a guided crisis-support framework helping parents navigate grooming, sextortion, or exploitation scenarios through evidence preservation, response workflows, and psychologically informed communication guidance.
- **GuidePost Conversational Co-Pilot** — a proactive communication support system designed to help parents maintain ongoing safety conversations through contextual prompts and educational nudges rather than direct surveillance.

Across these concepts, recurring themes included low-friction implementation, trust-centered intervention, AI-enabled guidance, and privacy-preserving safety architectures. The outputs highlighted how this segment values “supportive awareness” rather than punitive monitoring.

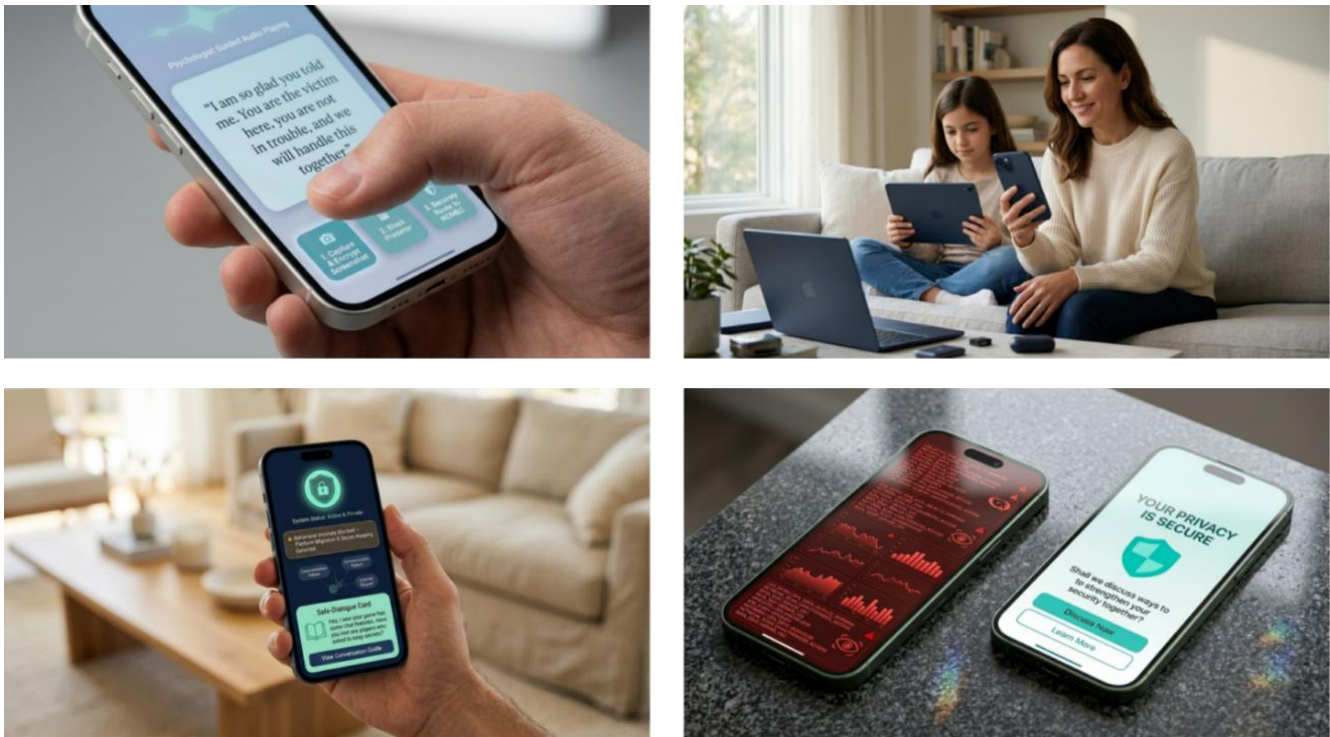


Figure 11 AI-Enabled Intervention for Pragmatic Balancers.

Vigilant Managers

For Vigilant Managers, the ideation process addressed a fundamentally different challenge: these parents strongly favored active oversight and robust controls but frequently experienced high levels of parent-child conflict and resistance to monitoring. The DesignThinker outputs identified what the system termed the “protection gap,” where increasingly restrictive surveillance behaviors often pushed children toward hidden or alternative digital environments.

The generated concepts focused on converting adversarial monitoring into transparent, collaborative protection systems:

- **Unified Device Trust Engine** — a bypass-resistant monitoring ecosystem integrating hardware-level attestation, encrypted synchronization, and contextual AI alerting across devices.
- **ContextShield AI Alerting** — a behavioral risk analysis layer designed to identify high-risk communication patterns without overwhelming parents with excessive alerts.
- **Collaborative Safety Governance Tools** — systems enabling shared family agreements, tiered permissions, and transparent accountability mechanisms intended to reduce family friction while maintaining strong oversight.

Unlike the Pragmatic Balancers concepts, these solutions prioritized enforcement reliability, ecosystem integration, and sophisticated technical controls. However, the AI synthesis repeatedly emphasized the importance of reducing emotional escalation and rebuilding trust within highly monitored households.

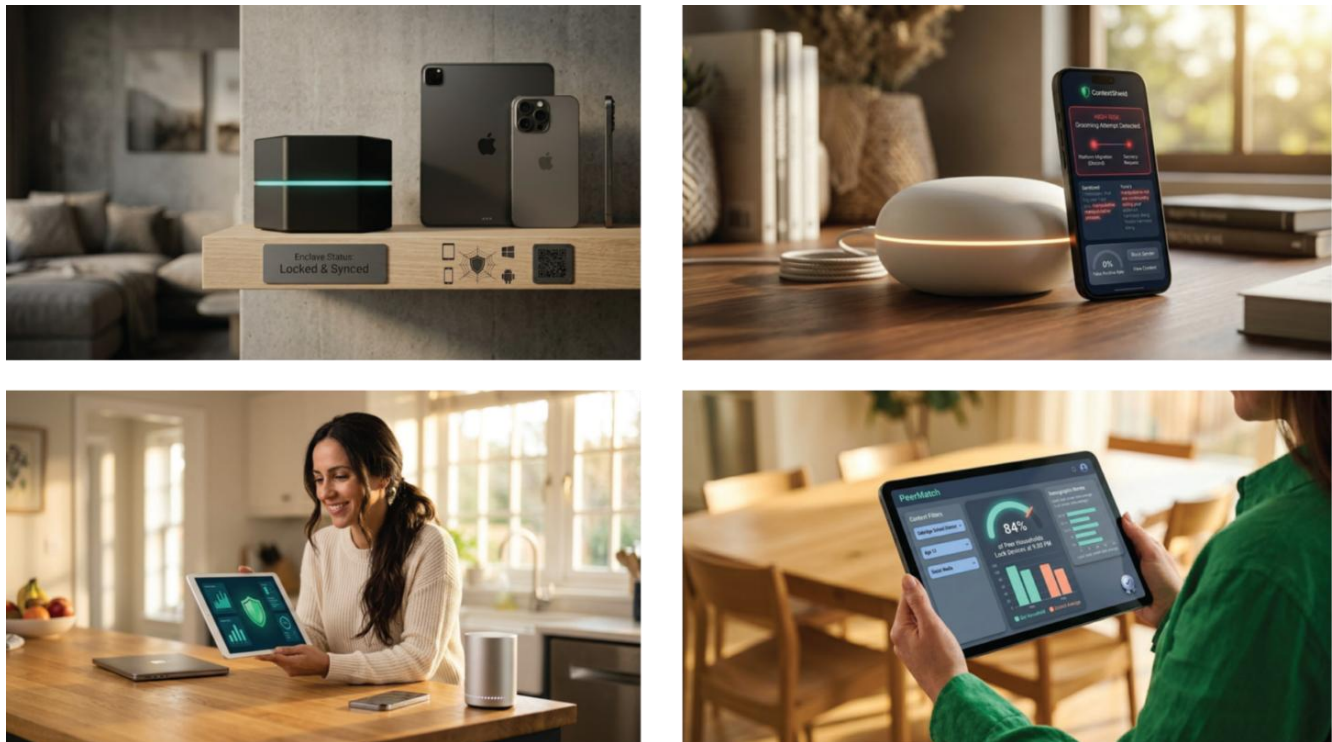


Figure 12 AI-Enabled Intervention for Vigilant Managers.

Social Risk Navigators

For Social Risk Navigators, the DesignThinker analysis identified a unique vulnerability profile centered on social and relational risks rather than technical or platform-based concerns alone. This segment reported lower technical confidence, inconsistent boundary enforcement, and heightened concern around peer influence, emotional manipulation, hidden communication channels, and online social dynamics.

The resulting concepts emphasized relational safety, communication transparency, and social-context awareness:

- **Unified Family Gating Profile** — a platform-agnostic safety orchestration layer translating complex privacy and communication settings into simplified relationship-centered guidance.
- **Safe Circle and Communication Mapping Tools** — systems helping parents understand evolving social ecosystems, trusted contacts, and behavioral relationship patterns without requiring invasive message access.
- **Crisis and Emotional Support Workflows** — guided parental coaching systems supporting conversations around cyberbullying, social coercion, exploitation, and emotional distress.

The AI-generated concepts consistently framed digital safety as a family communication challenge rather than purely a technical enforcement problem. Unlike other segments, the outputs emphasized emotional intelligence, social interpretation, and collaborative coaching over device control.

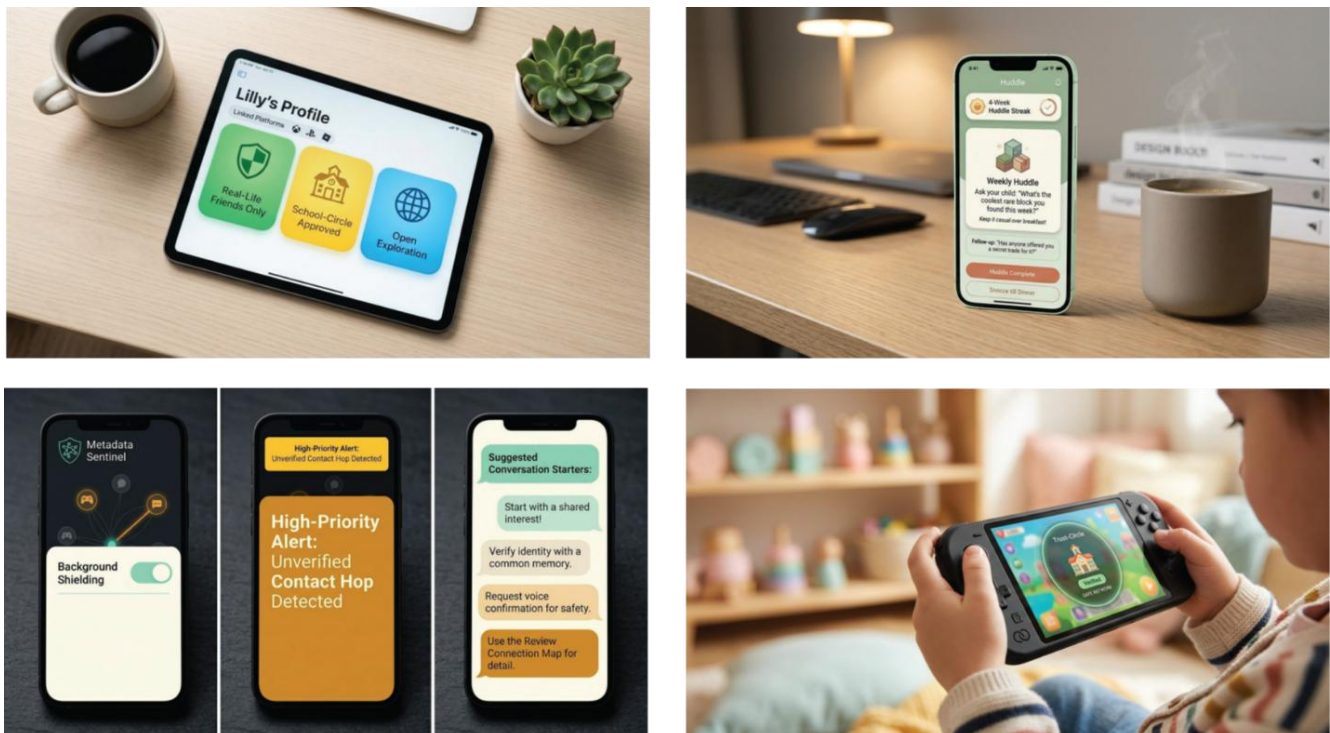


Figure 13 AI-Enabled Intervention for Social Risk Navigators.

Engaged Protectors

For Engaged Protectors (37% of parents), the DesignThinker process focused on solving the “surveillance dilemma.” These parents were highly engaged, technologically confident, and proactive about online safety, yet strongly opposed intrusive monitoring systems that undermined trust or adolescent autonomy.

The generated concepts centered on privacy-preserving intelligence and cooperative family safety:

- **Trust-Respecting Safety Telemetry** — a local, on-device behavioral risk detection system using semantic analysis to identify grooming, coercion, or exploitation patterns without exposing private communications.
- **Co-Navigation Frameworks** — systems encouraging collaborative parent-child digital safety conversations through shared insights, supportive prompts, and mutual visibility controls.
- **Incident Response Suite** — a guided support ecosystem designed for real-time crisis intervention while preserving child dignity, autonomy, and trust.

A defining theme across this segment was the rejection of traditional “spyware-style” parental monitoring in favor of cooperative, privacy-first safety architectures. The outputs also emphasized growing regulatory and societal pressures toward privacy-preserving child safety systems.

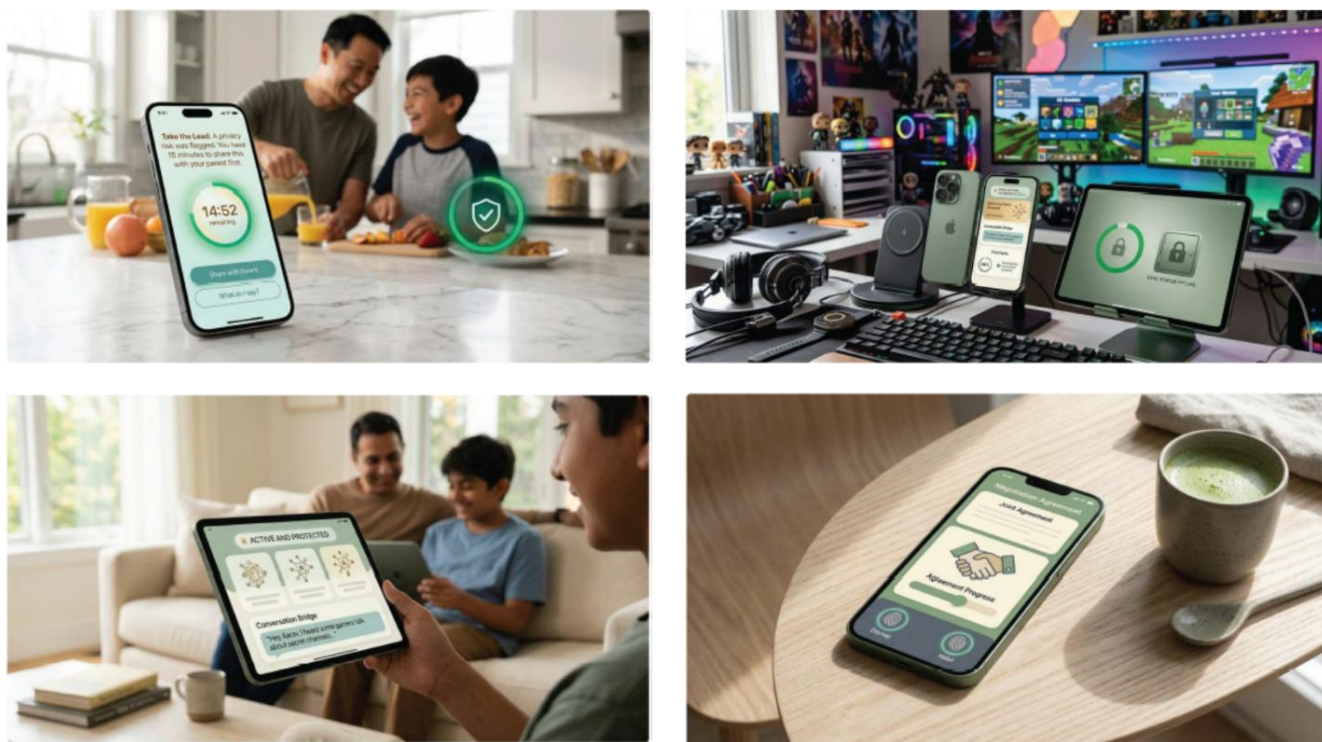


Figure 14 AI-Enabled Intervention for Engaged Protectors.

Cross-Segment Themes and Implications

Although the concepts differed substantially by segment, several cross-cutting themes consistently emerged from the AI-enabled synthesis process:

- shifting away from invasive surveillance toward collaborative safety models,
- increasing emphasis on privacy-preserving AI architectures,
- greater need for contextual and emotionally intelligent parental guidance,
- demand for low-friction implementation and family usability,
- and the importance of balancing protection with autonomy and trust.

Importantly, the DesignThinker outputs demonstrated how AI-enabled strategic synthesis can extend research beyond insight generation into highly tailored intervention design. Rather than producing generalized recommendations alone, the system translated segment-level behavioral and emotional patterns into differentiated conceptual solutions aligned to the realities of each parent population. This suggests that AI-supported synthesis platforms may represent a meaningful evolution in how segmentation research can inform product strategy, policy design, trust and safety systems, and digital wellbeing innovation.

Stakeholder Implications

Implications for Technology Companies

The data indicates that technology companies are facing a growing “protection gap” between the complexity of digital ecosystems and parents’ ability to manage online safety risks. Many parents report wanting stronger protection for children online while simultaneously expressing concerns about intrusive surveillance, loss of trust, and excessive monitoring.

The analysis also shows that parents are not a single audience. Different parent segments show substantially different preferences regarding monitoring and enforcement, communication and education, privacy and autonomy, and the role of AI-enabled safety solutions.

This leads us to the point that future online safety ecosystems may need to become more adaptive, configurable, and trust-centered rather than relying on one-size-fits-all control models.

The findings further highlight potential opportunities for AI-enabled safety systems, including:

- contextual risk detection,
- proactive guidance,
- privacy-preserving monitoring,
- and crisis-response support.

Additionally, successful implementation will likely require careful balancing of protection and privacy, automation and human judgment, and safety with parent-child trust and independence.

Overall, the research suggests that future child online safety solutions may increasingly require collaborative ecosystems involving technology companies, parents, schools, policymakers, and child-protection organizations rather than relying on any single stakeholder alone.

Implications for Educators and Schools

The findings identify the fact that educators and schools are playing an increasingly important role in children’s online safety ecosystems. Many parents reported relying on schools not only for digital literacy education, but also for reinforcement of online safety behaviors, cyberbullying awareness, and guidance around responsible technology use.

The research also identified a growing “protection gap” in which children’s digital experiences are evolving faster than many parents feel prepared to manage independently. This may create opportunities for schools to provide more consistent:

- digital citizenship education,
- online risk awareness,
- parent resources and guidance,

- and age-appropriate discussions around privacy, exploitation risks, scams, and healthy online behavior.

The findings also indicate that students may benefit most from approaches that combine education, communication, emotional support, and practical digital safety skills rather than relying solely on restrictive technology policies.

Finally, the segmentation results demonstrated that families differ substantially in their approaches to online safety, communication, and monitoring. This suggests that schools may benefit from flexible, family-centered approaches that recognize differing parent philosophies, technical confidence levels, and communication styles rather than assuming a single universal model of digital safety management.

Implications for Policymakers and Child Safety Organizations

The findings suggest that policymakers and child safety organizations are facing an increasingly complex online safety environment shaped by rapidly evolving technologies, fragmented digital ecosystems, AI-enabled interactions, and growing tensions between privacy, encryption, and child protection.

A key finding throughout the study was the emergence of a growing “protection gap” between parents’ awareness of online risks and their ability to consistently implement effective protections. This creates opportunities for policymakers and child safety organizations to support:

- clearer public guidance,
- accessible educational resources,
- digital literacy initiatives,
- and coordinated safety frameworks that help families navigate increasingly complex online environments.

The research also highlights the importance of balancing child protection, privacy, autonomy, and healthy digital development.

Parents consistently expressed discomfort with highly invasive surveillance approaches, so future child safety frameworks may need to prioritize transparency, trust-centered safety models, privacy-preserving technologies, and collaborative approaches involving families, schools, technology companies, and child-protection organizations.

Finally, the findings reinforce that online safety is not only a technology issue. It is increasingly a behavioral, educational, social, and governance challenge requiring cross-stakeholder collaboration and more adaptive approaches to prevention, intervention, and digital wellbeing support.

Implications for Parents and Families

Many families are navigating increasingly complex digital environments without feeling fully prepared to manage evolving online risks based on this research data. While most parents recognize meaningful concerns related to online safety, many also reported challenges balancing protection with trust, privacy, independence, and healthy communication.

Since the research reinforces that there is no single parenting approach to online safety, several themes consistently emerged as important across segments: ongoing communication, age-appropriate guidance, clear expectations and boundaries, and maintaining trust-based relationships around technology use.

The data also indicates that many parents may benefit from simpler, more practical support systems rather than highly technical or overly invasive monitoring solutions. Parents frequently expressed interest in tools and resources that reduce complexity, provide actionable guidance, support conversations with children, and help identify meaningful risks without requiring constant surveillance.

Finally, the study highlights that online safety is not solely about restricting access or monitoring behavior, but involves helping children develop:

- digital judgment,
- healthy online habits,
- awareness of risks,
- and confidence navigating digital environments safely and responsibly.

As digital ecosystems continue evolving, many families may benefit most from flexible, balanced approaches that combine protection, communication, education, and trust.

Implications for the Research Industry

This project raises broader implications for the future role of market research.

Research Beyond Measurement

A key objective of this project was to not stop at identifying concern levels or attitudes, and to help stakeholders determine where and how to take action. We believe that increasingly complex and ambiguous societal problems may require research approaches that also support:

- Strategy development
- Intervention planning
- Communication optimization
- Cross-stakeholder collaboration
- Actionable implementation pathways

This project illustrates a new way for research to evolve from passive observation toward enabling practical societal action.

AI as Research Augmentation Rather Than Replacement

The project also demonstrates how AI-enabled systems can augment research workflows when used responsibly.

Potential benefits include:

- Faster synthesis of large datasets
- Improved qualitative depth at scale
- Accelerated intervention ideation
- More efficient strategic development

At the same time, human agency, ethical review, contextual understanding, and methodological rigor remain essential.

Combining Quantitative Rigor With AI-Enabled Systems

A key methodological contribution of this project is the integration of:

- Traditional quantitative rigor
- Advanced statistical modeling
- NLP-assisted analysis
- AI-enabled strategic synthesis
- Human-centered interpretation

This hybrid approach represents an emerging direction for insight generation and implementation.

The Future of Socially Impactful Research

As organizations increasingly seek research with measurable societal outcomes, the industry may benefit from expanding its role beyond insight generation alone. This project demonstrates one possible model for how research can contribute more directly to societal impact.

Ethical Considerations and Responsible Use of AI

Given the sensitive nature of online child safety and exploitation topics, ethical safeguards were embedded throughout the project design, analysis, and interpretation process. The goal was to generate actionable insight while minimizing risk to respondents, avoiding sensationalism, and ensuring that AI-enabled methods were used as a responsible research aid rather than as an unchecked decision-making mechanism.

Sensitive-Topic Research Safeguards

The study was designed to protect respondents while still allowing parents and caregivers to share meaningful perspectives on a difficult subject. Safeguards included:

- **Respondent privacy and anonymity**, including reporting findings only in aggregate and avoiding personally identifiable details throughout the process
- **Careful sensitive-topic survey design**, using clear, non-graphic language and avoiding unnecessary detail that could be distressing or leading
- **Minimizing emotional distress**, including framing questions around parental concerns, preparedness, and support needs rather than asking respondents to recount traumatic experiences in detail
- **Responsible handling of open-ended responses**, especially where respondents described fears, perceived risks, or potentially sensitive child-related situations
- **Avoidance of fear-based framing**, ensuring that findings were used to clarify gaps and opportunities rather than amplify panic or stigma
- **Protection of vulnerable populations**, including careful interpretation of results related to children, families, and online exploitation risk

Responsible Use of AI-Enabled Methodologies

AI-enabled tools were used to augment the research process, particularly in synthesis, pattern recognition, and intervention ideation. They were not used as a substitute for researcher judgment, ethical review, or methodological rigor.

Safeguards included:

- **Extensive human testing and guidance for AI-probes** to open-ended questions to ensure follow-up probes were appropriate, focused, and not disturbing to respondents
- **Human review and validation of AI-generated outputs** before incorporating them into findings, implications, or recommendations
- **Researcher oversight at each stage**, ensuring that AI-supported synthesis remained connected to the research objectives, respondent data, and broader context

- **Transparency regarding where AI was used**, including distinguishing between survey findings, modeled results, AI-assisted synthesis, and researcher interpretation
- **Grounding all conclusions in observed data**, rather than allowing AI-generated concepts or narratives to become unsupported claims
- **Avoiding overstatement**, particularly around sensitive topics such as exploitation, grooming, parental preparedness, or child vulnerability
- **Reviewing AI outputs for bias, unsupported assumptions, or emotionally charged framing** before using them in deliverables
- **Using AI as an ideation and synthesis layer**, not as an autonomous analyst or final authority
- **Maintaining human responsibility for interpretation**, especially where implications involved children, family dynamics, privacy, autonomy, or potential intervention strategies

Practical and Ethical Balance

A central ethical challenge in this project was balancing the urgency of online child safety with the need to avoid overly invasive, punitive, or fear-driven responses. This was especially important because many parents are navigating a difficult tension between protecting children and preserving trust, privacy, autonomy, and healthy digital development.

For this reason, recommendations were developed with attention to:

- Whether proposed interventions could be implemented responsibly
- Whether solutions might unintentionally increase surveillance, conflict, or secrecy
- Whether communications could support constructive parent-child dialogue rather than fear or blame
- Whether AI-enabled outputs remained consistent with what the data actually supported

Summary Statement

This project demonstrates how AI-enabled research can be used responsibly in sensitive social-impact work when it is paired with strong human oversight, transparent methodology, careful interpretation, and clear ethical boundaries. The role of AI was not to replace the researcher, but to help accelerate and strengthen synthesis and broaden strategic exploration while preserving the core responsibilities of research: rigor, context, respondent protection, and evidence-based interpretation.

Conclusion

Children's online environments continue to evolve rapidly, creating both meaningful opportunities and increasingly complex safety challenges.

This research demonstrates that significant protection gaps exist between parental perceptions, child digital realities, and the broader ecosystem of online safety support.

The findings suggest that parents do not simply need greater awareness. They need clearer guidance, more practical tools, more actionable support systems, and solutions that acknowledge the complexity of balancing protection, trust, independence, and communication.

The project also demonstrates how advanced market research methodologies and AI-enabled systems can contribute to a more action-oriented research model.

By combining rigorous quantitative methodologies with AI-assisted synthesis and intervention development, research can seamlessly and quickly go beyond passive reporting toward enabling practical societal outcomes.

Ultimately, protecting children online will require coordinated efforts across families, educators, technology companies, policymakers, and child safety organizations.

Research alone cannot solve these challenges. However, thoughtfully designed insight systems can play an important role in helping stakeholders better understand risks, identify unmet needs, and accelerate more effective interventions.

References

- Common Sense Media. (2025). *Teens, Trust, and Technology in the Age of AI*. Common Sense Media. *Common Sense Media Research*
- Internet Watch Foundation. (2024). *Annual Report 2024*. Internet Watch Foundation. *Internet Watch Foundation Annual Reports*
- National Center for Missing & Exploited Children. (2024). *CyberTipline Reports*. NCMEC. *NCMEC CyberTipline Reports*
- OECD. (2024). *Children in the Digital Environment*. OECD. *OECD Digital Environment and Child Safety Resources*
- Ofcom. (2024). *Children and Parents: Media Use and Attitudes Report 2024*. Ofcom. *Ofcom Children and Parents Media Use and Attitudes Reports*
- Pew Research Center. (2024). *Teens, Social Media and Technology 2024*. Pew Research Center. *Pew Research Center Teens, Social Media and Technology Reports*
- Thorn. (2025). *Sexual Extortion & Young People: Navigating Threats in Digital Environments*. Thorn. *Thorn Research and Insights*
- Thorn. (2025). *Youth Perspectives on Online Safety, 2024: an Annual Report of Youth Attitudes and Experience*. Thorn. *Thorn Research and Insights*
- UNICEF. (2017). *The State of the World's Children 2017: Children in a Digital World*. UNICEF. *UNICEF Children in a Digital World*
- U.S. Department of Health and Human Services. (2023). *Social Media and Youth Mental Health: The U.S. Surgeon General's Advisory*. HHS Office of the Surgeon General. *U.S. Surgeon General Advisory on Social Media and Youth Mental Health*
- World Health Organization. (2024). *Adolescent Health*. World Health Organization. *WHO Adolescent Digital Health Resources*

Project Contributors

This project was developed through collaboration across research, strategic, analytical, and AI-enabled innovation disciplines.

Key contributors included:

SA Market Insights

- Joy Ganvik — Research design, methodology leadership, analysis, and paper development
- Carlos Salazar-Velasquez — Segmentation modeling and advanced analytics
- Kathy Schmitt — Project management and adaptive probing implementation
- Alexandra Tuleja — Strategic synthesis and intervention development
- Praveen Yadav — Project, field, and data management
- Pallavi Mittal — Visual design and report development
- Vinay Agrawal — Programming, quality assurance, and data processing

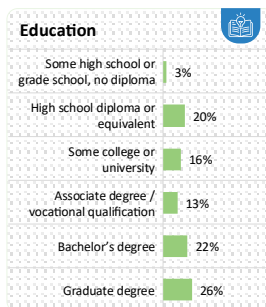
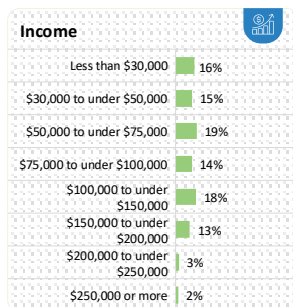
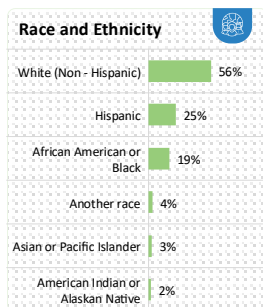
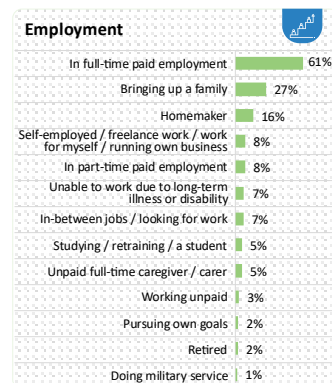
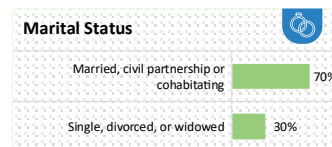
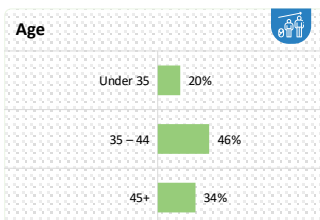
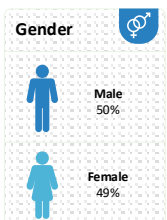
Amplifyer

- Anju Ahuja — Concept generation, scenario planning, and intervention ideation
- Justin Daab — AI platform development
- John Higginson — AI platform scalability

Appendix A: Sample Profile

Figure A1: Sample Composition: Parent

Sample Composition: Parent



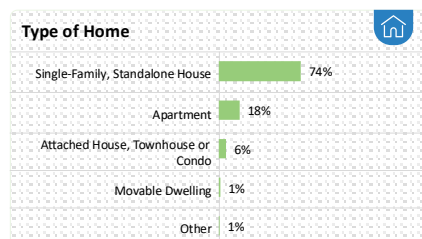
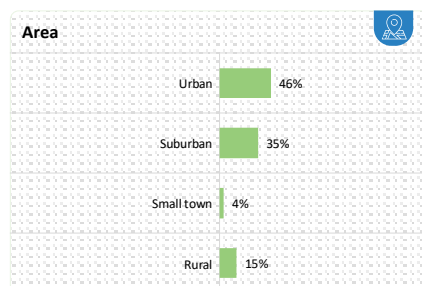
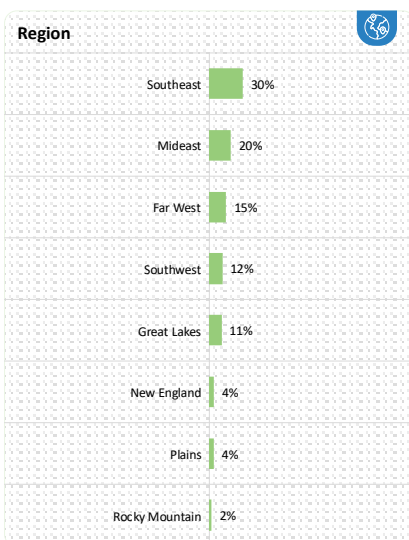
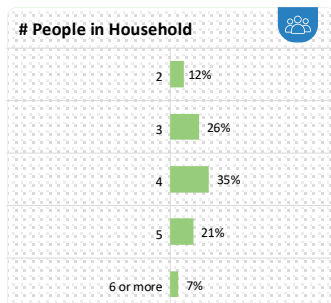
Base: Total - 1014
 S02. Please record your gender. S04. What is your age? S05. Which of these categories best represents your total yearly household income? S06. Are you from Spanish, Hispanic or Latino background / origin? S07. What is your race? D3. What is your marital status?
 D1. Which of the following describe you? D2. What is the highest level of education you have completed?

Copyright © 2026. SA Market Insights

197

Figure A2: Sample Composition: Household

Sample Composition: Household



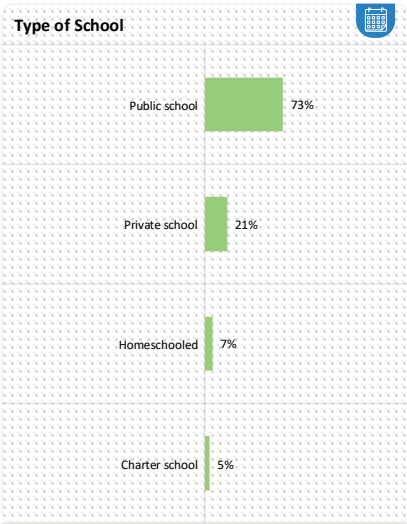
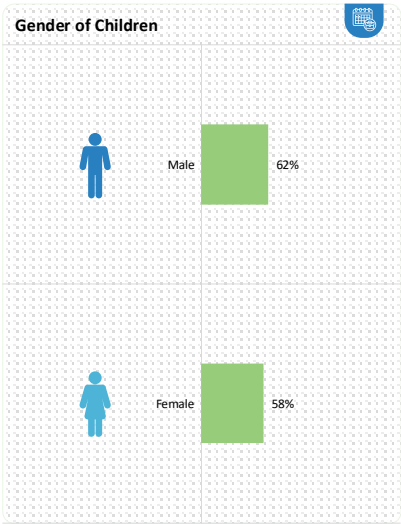
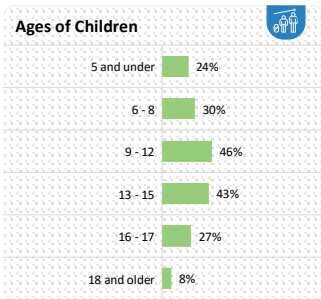
Base: Total - 1014
 S08. In which region of the country do you live? D6. Which best describes the type of area where you live? D7. In which type of residence do you live? D4. Including yourself, how many people live in your household?

Copyright © 2026. SA Market Insights

198

Figure A3: Sample Composition: Children

Sample Composition: Children



Base: Total - 1014
S10. What are the ages of the child(ren) in your household?, D8. Please record the gender(s) of the children in your household between the ages of 6-17, D5. What type of school(s) does your child(ren) attend?
Copyright © 2026. SA Market Insights

Appendix B: Segmentation Methodology

Latent class analysis (LCA) was selected because it allows respondents to be probabilistically grouped based on shared patterns across multiple attitudinal and behavioral dimensions rather than relying on distance-based clustering alone. This approach was particularly valuable given the overlapping and multidimensional nature of online safety behaviors, communication dynamics, and technology usage patterns.

Segment membership was incorporated into subsequent analyses including MaxDiff preference modeling, driver analysis, gap analysis, and AI-enabled intervention development to better understand how differing parent mindsets influence online safety priorities, preparedness, and solution expectations.

Multiple segmentation solutions were evaluated using a combination of statistical fit indicators, segment stability, interpretability, and practical differentiation.

The final four-segment solution was selected because it provided the strongest balance between statistical separation and meaningful behavioral differentiation across online safety attitudes, communication approaches, monitoring behaviors, and solution preferences.

Table A1: Fit Statistics

	Log-likelihood	Parameters	BIC	AIC	Iterations
6 Segment	-47,669.26	295	99,114.35	98,144.78	26
5 Segment	-48,309.03	246	98,320.79	97,110.07	25
4 Segment	-48,875.39	197	97,380.40	95,928.52	25
3 Segment	-49,667.14	148	100,358.69	99,630.29	15
BIC and AIC for the 4-segment solution are the lowest					

Appendix C: MaxDiff Design

MaxDiff prioritization modeling was used to identify which online safety features, interventions, and support mechanisms parents considered most important. The methodology enabled realistic prioritization by forcing trade-offs among competing features and solutions.

The final experimental design used included 14 choice exercises with 3 items shown per screen.

Final solutions included:

- **AI-Powered Monitoring and Detection:** Automatically scans messages and activity to detect risks like bullying, grooming, or inappropriate content
- **Real-Time Alerts and Notifications:** Immediately alerts parents when concerning behavior or interactions are detected
- **Parental Controls and Restrictions:** Lets parents block apps, limit access, and control what their child can do online
- **Contact and Communication Controls:** Limits who children can interact with and blocks unknown or suspicious contacts
- **Privacy and Data Protection:** Prevents sharing of personal information and ensures the child's data is kept secure and private
- **Content Filtering and Protection:** Blocks or filters inappropriate, explicit, or harmful content automatically
- **Activity Monitoring and Summaries:** Provides clear summaries of apps used, contacts, and overall online activity
- **Guided Support for Parents:** Gives parents clear recommendations and guidance on what to do when issues arise
- **Child Safety Education Tools:** Teaches children how to recognize risks and make safer decisions online
- **Parent-Child Communication Support:** Provides tools and prompts to help parents talk with their children about online safety
- **Emergency and Help Features for Children:** Includes SOS buttons and easy ways for children to report concerns or ask for help
- **Flexible Privacy and Control Settings:** Lets families choose the balance between monitoring and child privacy based on age or preference

Figure A4: Screenshot of MaxDiff Exercise

When it comes to solutions to help keep your child(ren) safe online...

Which are you MOST INTERESTED in? (Please select one)

Which are you LEAST INTERESTED in? (Please select one)

(Screen 2 of 14)

	Content Filtering and Protection	Contact and Communication Controls	Guided Support for Parents
	Blocks or filters inappropriate, explicit, or harmful content automatically	Limits who children can interact with and blocks unknown or suspicious contacts	Gives parents clear recommendations and guidance on what to do when issues arise
MOST	☒	☐	☐
LEAST	☐	☐	☒

< >

Clustering all twelve of the solutions areas identified an actionable 3-cluster solution: Hands-On Control, Balanced Safety, and Automated Protection.

Figure A5: MaxDiff Cluster Solution - Differentiating Solutions

CLUSTER 1 Hands-On Control 23%		CLUSTER 2 Balanced Safety 53%		CLUSTER 3 Automated Protection 24%	
Parental Controls and Restrictions - Lets parents block apps, limit access, and control what their child can do online	89%	Child Safety Education Tools - Teaches children how to recognize risks and make safer decisions online	64%	Real-Time Alerts and Notifications - Immediately alerts parents when concerning behavior or interactions are detected	89%
Privacy and Data Protection - Prevents sharing of personal information and ensures the child's data is kept secure and private	77%	Parent-Child Communication Support - Provides tools and prompts to help parents talk with their children about online safety	58%	Content Filtering and Protection - Blocks or filters inappropriate, explicit, or harmful content automatically	88%
Contact and Communication Controls - Limits who children can interact with and blocks unknown or suspicious contacts	64%	Guided Support for Parents - Gives parents clear recommendations and guidance on what to do when issues arise	37%	AI-Powered Monitoring and Detection - Automatically scans messages and activity to detect risks like bullying, grooming, or inappropriate content	86%
Emergency and Help Features for Children - Includes SOS buttons and easy ways for children to report concerns or ask for help	58%	Flexible Privacy and Control Settings - Lets families choose the balance between monitoring and child privacy based on age or preference	37%	Activity Monitoring and Summaries - Provides clear summaries of apps used, contacts, and overall online activity	44%
PROBABILITIES OF CHOICE					

Appendix D: Driver Analysis Modeling Details

To better understand what most strongly influences parents' sense of preparedness to manage online safety risks, driver analysis was conducted using Johnson's Relative Weights methodology.

The dependent variable measured perceived preparedness to prevent or respond to serious online safety risks, while independent variables included online safety mindset, technical confidence, use of safety tools, technology experience, and communication approach.

Johnson's Relative Weights (% of explained variance) was computed separately within each segment, using the 5 leading drivers. The fact that the top driver changes by segment is the key finding: preparedness is built differently in different segments.

Table A2: Driver Analysis

Segment	n	Model R ²
OVERALL (all parents)	1014	0.437
Pragmatic Balancers	413	0.316
Vigilant Managers	117	0.461
Social Risk Navigators	108	0.519
Engaged Protectors	376	0.384

Appendix E: Example AI-Enabled Probing Flows

AI-Powered Adaptive Probing: Illustrative Examples

The examples below illustrate several ways adaptive probing deepened or expanded the insights captured within the survey. We discovered during analysis that there were times that the AI-Generated Probe took the question in a slightly different direction. This proved to both confound and strengthen insights:

- we gained deeper insight around the question initially answered, or
- we learned about additional topics, not necessarily directly responding to the initial question, based on the parent’s initial response

Revealing Specific Risks and Threat Perceptions

In many cases, adaptive probing transformed broad statements about “online safety” into more detailed descriptions of the specific threats parents feared most. These follow-up probes helped surface concerns related to grooming, impersonation, scams, explicit content exposure, and exploitative interactions that were not fully articulated in the original responses.

Table A3: Revealing Specific Risks and Threat Perceptions

Initial Response	AI-Generated Probe	Expanded Insight
“I believe that she tries but really doesn't know what the risks are.”	“What specific risks do you think your child might not be aware of?”	“Bullying and sexually explicit pictures and content... adult themed pictures and movies that are available for anybody to come across.”
“They know the Internet and online world is a risky place.”	“How do you feel about the specific risks that your children face online, and what concerns you the most?”	“I worry about sexual predators or people misrepresenting who they say they are because online anybody can be anybody.”
“There are things and people out there today... just not trustworthy.”	“What specific online risks do you feel are the most concerning for your child?”	“Pedophiles disguising themselves as another kid or child his age trying to get him to meet up somewhere.”
“My child feels online safety rules are mostly fair, but sometimes restrictive.”	“What specific online risks do you feel are most important for your child to be aware of?”	“Talking to strangers online, sharing personal information, falling for scams, and being exposed to inappropriate content.”

Uncovering Parenting Philosophy and Trust Dynamics

The probes also revealed deeper parenting philosophies related to trust, independence, transparency, and balancing protection with autonomy. These themes often would not have emerged from the initial responses alone.

Table A4: Uncovering Parenting Philosophy and Trust Dynamics

Initial Response	AI-Generated Probe	Expanded Insight
“Teen resents monitoring but gets it.”	“How do you feel about balancing monitoring with respecting privacy?”	“More hands on with my 9-year-old, more trust and transparency with my 16-year-old.”
“My children trust me and I trust my children.”	“How do you think that trust impacts conversations about online safety?”	“This is a judgment-free zone... we're going to try and tackle a problem.”
“My oldest thinks it's a bit overprotective.”	“How do you personally view the online risks your children might face?”	“I keep an eye on things and talk with them, but I also know I can't watch everything.”
“They think I'm being overprotective.”	“How do you feel about balancing monitoring and privacy?”	“It's a tough balance. I want them safe, but I don't want to be overbearing.”

Identifying Practical Challenges and the “Protection Gap”

Several probes surfaced barriers that complicated parents' ability to consistently implement safety strategies. These responses provided important context around the broader “protection gap” identified throughout the research.

Table A5: Identifying Practical Challenges and the “Protection Gap”

Initial Response	AI-Generated Probe	Expanded Insight
“At first they didn't like it but then they saw what could happen.”	“What incidents or experiences made them recognize the importance of online safety?”	“Someone could see close location... it was quite scary for them and for us.”
“She thinks I'm a worry wart and annoying.”	“How do you feel about her perception of online risks?”	“That's why I do a quality check on her devices checking history, app usage, downloads, and messages.”
“I feel like it's my job to set controls up and prevent harm.”	“What are the main barriers that make it challenging to take protective actions?”	“My children are able to outsmart my safety measures... they can bypass locks and find disguised programs.”

Revealing How Children Interpret Online Safety Rules

The probes also helped uncover how children themselves interpret online safety restrictions, including what they find frustrating, what lessons resonate most strongly, and how their understanding evolves over time.

Table A6: Revealing How Children Interpret Online Safety Rules

Initial Response	AI-Generated Probe	Expanded Insight
"My child understands the rules but sometimes finds them annoying."	"What aspects of the rules do they find most limiting?"	"Screen time and restrictions from downloading some games."
"My daughter gets upset about the rules I have in place."	"How has your child's understanding of online safety evolved over time?"	"She's understanding there's other people she's interacting with and the dangers of the internet."
"My children understand the importance of online safety."	"What risks do you think they are most aware of?"	"Not sharing personal information, avoiding suspicious links, and cyberbullying."

Surfacing Real Monitoring Behaviors and Safety Strategies

Finally, adaptive probing frequently transformed broad claims about "monitoring" into more detailed descriptions of actual household safety practices, layered monitoring approaches, and real-world supervision strategies.

Table A7: Surfacing Real Monitoring Behaviors and Safety Strategies

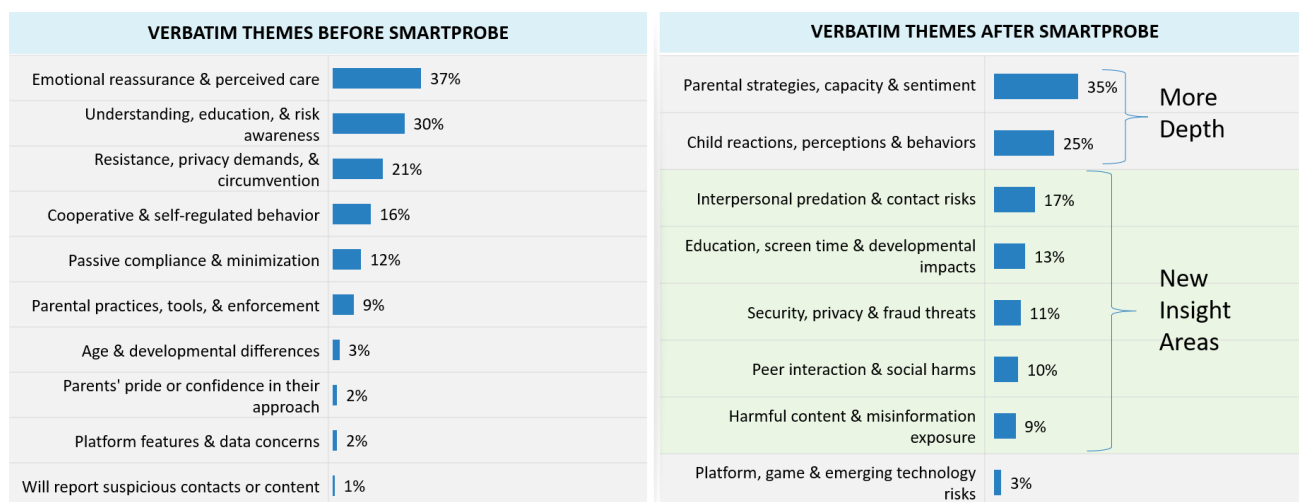
Initial Response	AI-Generated Probe	Expanded Insight
"My kids understand why I monitor their online activity."	"What monitoring practices do you find most effective?"	"Open conversations, parental controls, keeping devices in common areas, and occasional check-ins."
"I closely monitor what they are doing."	"What strategies do you use to monitor online activities, and how effective have they been?"	"They are only allowed certain apps with supervision... going over with them anything I see and hear and don't like and why."

Appendix F: NLP-Assisted Verbatim Analysis

To further evaluate the value of AI-powered adaptive probing within the survey, NLP-assisted verbatim analysis was conducted comparing themes identified from respondents' initial open-ended responses versus the expanded responses generated after AI-powered follow-up probing. The comparison demonstrated that the adaptive probes consistently increased the depth, specificity, and contextual richness of the insights captured. Initial responses frequently reflected broad or generalized concerns related to “online safety,” “monitoring,” or “trust,” while the AI-probed responses surfaced substantially more nuanced themes including grooming concerns, impersonation risks, scams, explicit content exposure, privacy tensions, trust dynamics, emotional reactions, implementation barriers, and evolving parent-child communication strategies.

The analysis also revealed that adaptive probing frequently transformed short attitudinal statements into more behaviorally and emotionally detailed narratives. In many cases, the AI-generated probes uncovered practical examples, specific incidents, real-world parenting strategies, and underlying motivations that would likely not have emerged through traditional open-ended questioning alone. This supports the broader methodological finding that AI-enabled probing may help bridge the gap between quantitative scale and qualitative depth by generating richer contextual understanding while maintaining the scalability and structure of large-sample survey research.

Figure A6: Verbatim Theme Comparison Pre and Post Smart Probe



Base: Total - 1014
 R6. How does your child(ren) feel about efforts to keep them safe online?

Appendix G: Example Amplifyer Intervention Concept

The following example illustrates the type of output generated using the Amplifyer DesignThinker framework — a structured AI-enabled innovation process designed to rapidly transform research insights into actionable product concepts, positioning frameworks, and visualized solution narratives.

In this example, the system identified an unmet need among a specific parent segment referred to as “Social Risk Navigators” — parents concerned about online grooming, predatory contact, and inappropriate peer interaction, but who are uncomfortable with invasive surveillance-based parental control tools. The research highlighted a major “protection gap,” where parents wanted stronger interpersonal safety controls but lacked the technical confidence to navigate complex platform privacy settings and communication restrictions.

Using these insights, DesignThinker synthesized findings into a fully developed product ecosystem centered around “One-Touch Gating,” a simplified, privacy-preserving digital safety platform. The resulting output included:

- Clearly defined target audience and unmet need
- Product concept generation and prioritization
- User journey mapping and safety workflow design
- Naming, positioning, and messaging frameworks
- Visualized product interfaces and interaction concepts
- Go-to-market and investor-oriented storytelling assets
- TAM framing and strategic differentiation

The process incorporated multiple stages of iterative AI-supported ideation, concept refinement, narrative development, and visual generation. Outputs included realistic product renderings, interface concepts, dashboard flows, ecosystem diagrams, pitch deck slides, and implementation frameworks designed to simulate the type of strategic deliverables typically created through cross-functional workshops involving research, UX, product strategy, and innovation teams.

The resulting concept demonstrated how Amplifyer DesignThinker can accelerate the transition from research insight to tangible innovation direction — compressing what traditionally requires weeks of collaborative concept development into a rapid, structured workflow while maintaining strategic coherence, audience specificity, and presentation-ready outputs.

This example is intended to illustrate the breadth, depth, and practical applicability of AI-enabled concept generation within a market research and innovation workflow.

Appendix H: About SA Market Insights

SA Market Insights is a global custom market research and strategic insights firm specializing in quantitative and qualitative research, advanced analytics, segmentation, and innovation-focused insight development. The company works with organizations across technology, software, telecommunications, energy, and other industries to support product strategy, positioning, customer understanding, and market opportunity identification.

The firm combines primary research rigor with emerging AI-enabled methodologies, including advanced statistical modeling, NLP-assisted analysis, adaptive qualitative probing, and AI-supported strategic synthesis. SA Market Insights focuses on translating complex research findings into actionable business and societal insights through practical, decision-oriented research approaches.

Appendix I: About Amplifyer

Amplifyer is an AI-native Human-at-the-Helm platform built for Product, Marketing, Insights, Operations, Strategy, Sales and Finance functions to solve strategic problems. Amplifyer augments intelligence and accelerates discernment by subject matter experts. It helps organizations more rapidly operationalize strategic insights and market intelligence. Amplifyer was designed to increase human agency by accessing a wide swath of intelligence, processing vast arrays of insights, performing extensive time-consuming strategic analysis using codified frameworks and best practices, conducting a rigorous design-thinking process to develop solution prototypes, simulate insights based on these prototype concepts, and finally spinning up a virtual marketing team to develop marketing, PR, branding and communication strategies. Amplifyer's apps are targeted to serve the analyst, the executive and other key stakeholders.

From its inception in early 2024, Amplifyer's AI-native platform uses a human-centric approach to strategic work spanning core business functions. Amplifyer is unique in many respects from direct interactions with platform AI companies (Gemini, Claude, ChatGPT, Perplexity) as well as in-house systems using their own models in the following ways:

- **Design:** Amplifyer implements codified best practices for research, problem identification and definition, hypothesis formulation, strategic analysis, solution development, and the generation of communications strategies. Amplifyer's hundreds of agents are designed and tested to perform discrete aspects of complex, detailed, and highly managed tasks, from data gathering, framing, hypothesis formulation, analysis, fact checking and verification, synthesis, design and reporting.
- **Technology:** Amplifyer is powered by the Google Gemini suite of LLMs. After more than a year of testing, when paired with Amplifyer's structured processes, Gemini proved to have an unmatched ability to provide sophisticated and robust results to strategic problems. Amplifyer leverages Google's latest models with advanced capabilities in its stack, including real-time grounded search to gather data and market intelligence that lives outside of the model and is critical to the analysis at hand, including up-to-the-minute data from the Web. Google Research also enables verification of sources, and attributions. Amplifyer is full-stack Google, leveraging a suite of Google solutions to provide a seamless experience and scalable solutions. Amplifyer is a proud member of the Google Startup Accelerator program.
- **Privacy:** Amplifyer has been designed as a privacy-first platform, due to the sensitive nature of queries and proprietary data analyzed by its privately-held and publicly-traded customers. Amplifyer has no visibility into user interactions with the tools, other than basic account credentials and payment information, and no user interactions are ever used to train the underlying LLM.
- **Usability:** Amplifyer has been designed with an interface that is easy to navigate for beginners and sophisticated enough for power users to create their own workflows.
- **Outcomes:** Amplifyer was created by leaders and subject matter experts in strategy, innovation, product, insights, marketing and technology. Logic and technique is documented for the user, including pedagogical context where appropriate, while generating executive-level output for leadership. Amplifyer's results have been tested against other methods of directly engaging with

LLMs, including ChatGPT, Claude, and interacting with Gemini directly, and consistently delivers deeper analysis, more unique, robust, and insightful strategies, and actionable recommendations, including implementation plans. Case studies illustrate how Amplifyer augments human and team performance across verticals and problem types.

Unlike traditional AI tools focused primarily on content generation, Amplifyer is designed to support end-to-end strategic workflows — combining insight synthesis, innovation development, future scenario planning, and guidance within a structured multi-agent environment.

Core Capabilities

Strategic Insight Synthesis

Amplifyer can rapidly synthesize large volumes of structured and unstructured data, including survey findings, segmentation outputs, verbatim responses, trend signals, and behavioral patterns.

The platform helps identify emerging themes, unmet needs, strategic risks, and opportunity areas that may not be immediately visible through traditional reporting approaches alone.

Multi-Agent AI Collaboration

Amplifyer uses proven processes that leverage coordinated AI “agents” that simulate different strategic perspectives and disciplines, such as research, behavioral science, UX design, communications, product strategy, and innovation planning. This allows the platform to support more holistic and interdisciplinary solution development.

Concept and Intervention Development

The platform can generate:

- market intelligence
- stakeholder simulations
- product and service concepts,
- intervention strategies,
- communication campaigns,
- stakeholder engagement frameworks,
- educational approaches,
- and implementation pathways

based directly on research findings and audience needs.

Futurecasting and Scenario Planning

Amplifyer supports future-oriented strategic thinking by generating plausible future scenarios, emerging risk trajectories, ecosystem shifts, and long-term strategic implications to help organizations prepare for evolving environments.

AI-Enabled Storytelling and Communication Optimization

The platform can tailor communications, narratives, and visual concepts to different stakeholder audiences while aligning messaging to audience psychology, motivations, and communication styles.

Making Research Actionable

One of Amplifyer's core value propositions is its human-at-the-helm design to help organizations use one shared intelligence platform to move beyond insight generation alone by supporting:

- strategy development,
- roadmap creation,
- stakeholder alignment,
- prioritization,
- and action-oriented implementation planning.

Amplifyer illustrates how AI-enabled strategic intelligence platforms can help transform research from passive insight generation into actionable strategy, intervention development, and operational decision support while maintaining human-centered oversight and methodological rigor.

We hope
you can
help build
the future
with us



Joy Ganvik, CEO, SA Market Insights

jganvik@samarketinsights.com

Anju Ahuja, Co-Founder and COO, Amplifyer

anju@amplifyer.ai



SA MARKET
INSIGHTS Amplifyer

