



A latent profile analysis of dyadic level information disclosure behaviours: an investigation of parent-teen dyads

Robert E. Crossler, France Bélanger, Katherine R. Allen & Julia Stachofsky

To cite this article: Robert E. Crossler, France Bélanger, Katherine R. Allen & Julia Stachofsky (16 Mar 2026): A latent profile analysis of dyadic level information disclosure behaviours: an investigation of parent-teen dyads, Behaviour & Information Technology, DOI: [10.1080/0144929X.2026.2642836](https://doi.org/10.1080/0144929X.2026.2642836)

To link to this article: <https://doi.org/10.1080/0144929X.2026.2642836>



Published online: 16 Mar 2026.



Submit your article to this journal [↗](#)



View related articles [↗](#)



View Crossmark data [↗](#)



A latent profile analysis of dyadic level information disclosure behaviours: an investigation of parent-teen dyads

Robert E. Crossler ^a, France Bélanger ^b, Katherine R. Allen ^c and Julia Stachofsky ^d

^aDepartment of Management, Information Systems, and Entrepreneurship, Washington State University, Pullman, WA, USA; ^bDepartment of Accounting and Information Systems, Virginia Tech, Blacksburg, VA, USA; ^cDepartment of Human Development and Family Science, Virginia Tech, Blacksburg, VA, USA; ^dDepartment of Business Information Systems, Western Michigan University, Kalamazoo, MI, USA

ABSTRACT

Information disclosure decisions often have impacts beyond just the person who made the decision to share the information. This is especially true for family members, where one family member's decision to share information can result in a privacy breach that affects the entire family. However, few studies have examined information disclosure decisions when more than one person is affected. This research uses a latent profile analysis of parent-teen dyads to understand collective information disclosure decisions via the use of technology that may affect the entire family. To conduct the study, we surveyed dyads of a parent and a related teenager at two points in time regarding their perceptions and intentions to share information via an app that may affect other family members, including those outside the dyad. The latent profile analysis revealed two types of parent-teen dyads: technology-resistant and technology-receptive. We conceptualise these empirically derived privacy profiles as relational orientations toward collective privacy, demonstrating how latent profiles can be theoretically interpreted as outcomes of ongoing social and relational processes within dyads. We highlight how future research can leverage latent profile analysis to obtain a deeper understanding of dyadic-level decisions, such as information disclosure.

ARTICLE HISTORY

Received 17 September 2025
Accepted 3 March 2026

KEYWORDS

Privacy; profile analysis; information disclosure; privacy calculus; dyads

1. Introduction

Individuals regularly decide what information to reveal. These decisions are often evaluated based only on how they may affect the self. However, the impacts of a privacy decision are rarely confined to the individual making it. Decisions to share information or use technologies that require disclosure may compromise the privacy of everyone within an individual's social groups. These decisions are instances of interdependent privacy (Franz and Benlian 2022; Zhang and Zhu 2025), in which an individual's decision affects others' privacy. For example, approximately 90% of households can be identified using one family member's postal code and birthdate (Patterson 2021), and yet some of this is co-owned information – information about multiple people (Zhang, Turel, and Zöll 2026). However, existing research predominantly focuses on individual-level decisions. Investigating collective information disclosure decisions is essential because these decisions often involve complex interactions between individual and collective privacy concerns. For instance, a parent's decision to use a family tracking app may conflict

with a teenager's desire for privacy. Understanding these dynamics is vital for developing technologies and policies that respect and protect family privacy. We ground our analysis in the privacy calculus model, which posits that individuals' information disclosure decisions are partially informed by their estimates of the costs and benefits of making privacy decisions (Bélanger, Crossler, and Correia 2021).

In this paper, we report on a study that uses a latent profile analysis to examine how data from a parent-teen dyad can be used to demonstrate the consistency of decision-making within a collective (i.e. dyad) and predict individual intention. Dyads represent related (or social) groups of two distinguishable individuals (Kenny, Kashy, and Cook 2006; Zöll, Franz, and Turel 2026), in this case, a parent and a teen, as a subset of a larger family unit. Latent profile analysis is a method for identifying theoretically interesting subpopulations that are often overlooked by aggregation-based methods (Mattke et al. 2018; Spurk et al. 2020). This method moves beyond the assumption that individual measures capture the perspectives of all members of a dyad, which

can lead to inaccurate conclusions. By considering multiple perspectives within a collective, this study provides a more comprehensive understanding of information disclosure decisions. Failing to investigate collective decisions about information disclosure can have significant consequences, including privacy breaches¹, family conflicts², and the development of technologies that do not adequately protect family privacy.³ This study aims to mitigate these risks by providing insights into the collective dynamics of information disclosure within families. Drawing on the privacy calculus, well established as a theoretical framework at the individual level of analysis (Bélanger, Crossler, and Correia 2021; Dienlin 2023; Trepte, Scharkow, and Dienlin 2020), we extend it to incorporate joint evaluations of risk and benefits that emerge from shared, collective privacy orientations among parents and teens. This extension offers a conceptual foundation for developing more robust group-level theorising around privacy.

Existing challenges, such as the privacy concerns raised by using contact-tracing apps during the COVID-19 pandemic (Whitney 2020), underscore the need for further research into collective decisions about information disclosure. Survey findings indicate that privacy concerns are a significant barrier to adopting such technologies, underscoring the importance of understanding and addressing them within family contexts (Chan and Saqib 2021). How these collective concerns shape technology use decisions is essential for designing interventions, policies, and tools that effectively support privacy protection at the family level.

Exploring collective privacy addresses level bias, a long-standing bias in privacy research (Bélanger and Crossler 2011; Smith, Dinev, and Xu 2011). Level bias is created by failing to examine privacy decisions at any level beyond the individual level (Burton-Jones and Gallivan 2007). This bias occurs because the individual level is so heavily emphasised that the relationship between privacy assessments and decisions is inadequately recognised at other levels. This lack of knowledge accumulation regarding dyadic-level decisions prevents understanding what determines collective-level information-sharing behaviours. Ultimately, this can result in multiple multilevel fallacies (Bélanger et al. 2014), including the cross-level fallacy, the contextual fallacy (i.e. failing to consider higher-level moderators of the antecedents and consequences), the ecological fallacy (i.e. overgeneralising a relationship from higher levels to a lower level), and the atomistic fallacy (i.e. assuming the generalizability of a lower-level relationship to a higher level). Recognising and correcting these fallacies is essential for developing a more nuanced, multilevel understanding of privacy

dynamics, particularly within family systems where privacy-related decisions often involve interdependent actors.

Given the issues with prior privacy research at the individual level, our research is guided by the following question: *How do configurations of interdependent privacy perceptions held by parents and teens in a parent-teen dyad influence their information disclosure decisions via technology usage?* To conduct the study, we collected privacy calculus-based perceptions and information disclosure intentions from 109 dyads of parents and their teens at two time points. We used the data to create profiles and examined how they changed over time. This exploratory study provides novel insights into the longitudinal decision-making process for dyads, using a latent profile analysis (Lazarsfeld and Henry 1968; Spurk et al. 2020). We demonstrate the value of a latent profile analysis for studying collective privacy orientations that emerge from interdependent individual perceptions by identifying theoretically meaningful dyadic subpopulations that remain obscured when data are aggregated at the individual level.

First, we present background literature on information privacy, information disclosure decisions within collectives, and the privacy calculus, and extend this literature to families. We then describe how we conducted the study and performed a latent profile analysis to categorise parent-teen dyads based on their perceptions regarding using an app that requires information disclosure. Finally, we discuss the implications of the study's findings on privacy research within a collective before offering concluding comments.

2. Background

Limited empirical research exists that studies decision-making behaviour beyond an individual (Kenny, Kashy, and Cook 2006), especially regarding information sharing decisions (Bélanger and James 2020). Group-level research allows for investigating interpersonal interactions and relationships in ways not possible with individual-level research. Although research is often conducted at the individual level, phenomena explored in information systems behavioural research are often not exclusively about an individual, but instead about an individual's interaction with others embedded in the same social context. Dyadic relationships provide a foundational means for exploring these interrelations (Kenny, Kashy, and Cook 2006), helping researchers avoid the problem of pseudo-unilaterality, where it is assumed that the individual measure captures both people's perspectives (Duncan et al. 1984). By recognising dyads as interdependent units rather than mere

collections of individuals, researchers can better capture the relational processes that shape privacy-related decisions.

According to Kenny, Kashy, and Cook (2006), a key factor in dyadic relationships is the lack of independence between the two members of the relationship. This means that two people do not represent individual viewpoints but instead have something in common. This nonindependence arises from various linkage types, including voluntary linkage, kinship linkage, experimental linkage, and yoked linkage. Voluntary linkages are represented by friends or dating couples who choose to be in those relationships. Kinship linkages are represented by family members. Experimental linkages are represented by relationships in a laboratory environment where participants are forced to get to know one another. Yoked relationships involve people who never knew each other but are linked because of similar interactions, such as two patients of the same doctor. Multiple linkages may also influence people. An example would be a spousal relationship with both voluntary and kinship linkages. Across these linkages, the relational context of the dyad can shape the individuals' perceptions and views because of what is shared (Kenny, Kashy, and Cook 2006). Another important characteristic is distinguishability, where members may differ in systematic, identifiable ways. For example, siblings may be distinguishable by their age, while identical twins may be indistinguishable despite also being siblings. This current research relies on the kinship linkage of a distinguishable relationship between a parent and their teenager.

2.1. Information disclosure decisions in dyads

Parents and teens form an important dyadic relationship in which these family members have a kinship linkage, such that their perceptions are no longer independent. Given the distinguishable nature of this relationship, however, they may have differing views regarding technology use and information disclosure. The process in which two or more individuals are affected by one's disclosure of information captures a decision-making process that has rarely been studied within the privacy literature (Bélanger and James 2020). Prior research also suggests that family decisions are more complicated than simply being an aggregation of individual decisions, given the generational power differences, intense communications and interactions, and the expectation of permanence that characterise families (Allen and Henderson 2023; Daly 2003). Human relationships, especially in families, are complex and variable. As such, studying how people interact as

family members requires considering inevitable variations and changes over the life course (Allen and Henderson 2023). These dynamics create opportunities for conflict, negotiation, and adaptation as family members navigate differing beliefs, needs, and expectations around privacy and technology use. If an individual family member's information privacy decisions are made based on this individual's beliefs, the decision may not be consistent with what other members of the family would do (Bélanger et al. 2022).

To anchor this work, we rely on the privacy calculus model, a common theoretical lens used to explore information privacy decisions and intentions (Bélanger and Crossler 2011; Smith, Dinev, and Xu 2011). Research on information privacy concerns within the family has accelerated in the last decade (Hertlein and Twist 2019). For example, with the use of virtual classrooms, some background behaviours in the homes of students have been recorded with school and criminal disciplinary actions occurring as a result of observed home behaviours, such as toy guns being used to play within the home, resulting in the adolescent being suspended and having a criminal record as a result of an invasion of the family's privacy (Shkedy 2020). Further family-related privacy issues have arisen as people pursue genealogy-related information through services such as 23andMe. Use of this service has led people to identify an unknown parent or other family members who never consented to have their information shared (Romine 2021). These illustrate the growing salience of information privacy concerns within families. Such concerns also highlight that family privacy issues long predate the digital era (Petronio 2010), though contemporary technologies have amplified their scope and consequences (Arıcı 2021).

While the privacy calculus has been extensively used at the individual level of analysis, few studies have included it at other levels. Some exceptions include studies leveraging the calculus to examine dyadic, interdependent, and collective privacy contexts. For example, in a study examining information disclosure on social media about others, both the benefits and risks to the self and others were considered. The results show that the interdependent "self-other" privacy calculus is supported (Zhang and Zhu 2025). This conceptualisation is consistent to how the calculus is used in the present study. Another study focused on interdependent privacy, focusing on co-owned information on social platforms, measures the effects of self, other's, and relationship benefits perceptions on disclosure decisions (moderated by co-owned information perceptions) finds that the self and collective benefits perceptions do increase disclosure by improving perceived

distributive fairness for both parties (Feng et al. 2025). At the collective level, the calculus has been measured as a collective privacy calculus to examine its influence on disclosure of co-owned information. It specifically considers collective privacy concerns and a collective calculus as mediators between impression management motives and disclosure decisions, where benefits and risks are for the relationship between individuals (Feng, Zhang, and Li 2023). While overall there are few studies that have examined the calculus at a level beyond the individual level of analysis, these studies collectively demonstrate that information disclosure decisions can be influenced not only by individual perceptions of cost and benefits to the self, but also by shared or interdependent evaluations of these in consideration of others' privacy, fairness, and relationship-level outcomes.

Our research uses family information privacy decisions as an exemplar for dyadic data analysis. However, given the complex relationships within families, we selected and empirically explored one meaningful relationship in which differential power exists, that of a teen and their parent or guardian. This differential of power means that there is a possible negotiation or even tension regarding the use of technology or its related decisions (Dworkin 2018). Thus, the distinguishability of members within this dyadic relationship should be evident (Kenny, Kashy, and Cook 2006). Although dyads have been used sparingly in information systems research, for example, to explore decision-making between project managers and supervisors (Iacovou, Thompson, and Smith 2009), they are valuable for capturing interdependent decision processes. We included teens rather than younger children because privacy decisions related to app use require a smartphone. Research has also shown that younger children may not have the cognitive capabilities to understand information disclosure decisions well (Hiller et al. 2008). The power differential means that typically, a parent decides whether to purchase a smartphone for their teen; however, they may have limited control over how the teen uses it. Although the parent-teen dyad does not fully represent the diversity of family structures and relational dynamics, it provides a useful proxy for understanding technology-related information privacy decisions within families. Using dyadic data allows us to explore both alignment and divergence in parent and teen perceptions through the lens of the privacy calculus.

2.2. Privacy calculus

Substantial research has shown that the privacy calculus helps explain an individual's willingness to share

information or intention to use a technology that requires sharing information (Dinev & Hart, 2006; Li 2012; Xu et al. 2010). This foundational privacy view has been primarily as self-centric instead of others-centric (Zhang and Zhu 2025), where individuals' information disclosure decisions are partially informed by their evaluations of the costs and benefits of making that decision, with perceived benefits often being the strongest component (Bélanger, Crossler, and Correia 2021). While our study extends this view by incorporating others' privacy considerations, the underlying logic remains similar: people engage in a cost-benefit evaluation that encompasses both their own and others' outcomes. This expanded perspective aligns with the "self-others calculus," which accounts for how individuals weigh risks and benefits not only to themselves but also to people connected to them (Zhang and Zhu 2025). As such, we conceptualise dyadic privacy calculus as a reflection of an interdependent configuration of individual privacy perceptions that emerged from ongoing interaction, mutual influence, and shared context within the dyad.

In this study, the benefits of releasing information through an app can be viewed as health-related (e.g. determining whether to be tested or quarantined) and convenience-related (e.g. the ability to attend work or school or visit family members). Benefits are generally specific to the technology or service of interest, such as deciding to participate in a transaction based on the expected outcomes (Ozdemir et al. 2017). Similarly, numerous studies have included perceived risks or privacy concerns as core components of the cost side of the calculus (Bélanger and Crossler 2011; Smith, Dinev, and Xu 2011). Accordingly, we measure privacy concerns with disclosing information through an app, but extend the concept to include both concern for the self and concern for others in the family. This dual focus enables us to capture the interdependent nature of family privacy, in which individuals may evaluate risks in terms of both personal vulnerability and potential harm to others within the household.

In past research, the privacy calculus has been used to examine individual behaviours, such that a family member ultimately makes information-sharing decisions within the family. However, individual decisions may affect other family members, similarly to other collectives, such as when employees' decisions affect their workgroup (Bélanger and James 2020). The key question, however, is whether these decisions can reflect the characteristics of a family, such that a type of family relationship can emerge in which individuals are either in sync with each other's perceptions or out of sync. There is limited empirical research in this domain,

except for theoretical models of how individuals make decisions while embedded in social groups (Bélanger and James 2020; Laufer and Wolfe 1977; Petronio 2013).

3. Methodology

We collected longitudinal data through two surveys administered to parent-teen dyads over six months. The data were analysed to create profiles of the dyads at Time 1 and Time 2. As explained earlier, parent-teen dyads are one type of family relationship in which there is an intergenerational power differential, yet both participants can own a smartphone (a requirement for our study).

The context utilised in this study was the release of information by using a contact tracing app (CTA). The technology was meant to help curtail the spread of COVID-19 during the pandemic, but public understanding of its function was often limited (Ladyzhets 2021). For this technology to work correctly in protecting communities, 80% of smartphone owners needed to use it (Servick 2020). However, heightened privacy concerns limited the apps' adoption and, thus, their effectiveness in protecting individuals, families, and communities. In fact, 71% of adults stated they were unwilling to use such a CTA due to privacy concerns (Whitney 2020). However, when people were provided information about other people who have been diagnosed with COVID-19, they were more likely to use CTAs (Ghose et al. 2024). This situation provides an interesting contradiction where people are not willing to use the app for their own privacy reasons but are willing to use the app if others give up their privacy. Regardless of how the CTA works, individuals' perceptions can create barriers to adoption, and in this case, they believe that if one person is tracked through a CTA, the other could also be tracked. For example, if a parent and teenager went on vacation and one of them had the CTA enabled, the other person was functionally traceable. Yet, the parent and the teen might not have the same beliefs towards privacy and information sharing, resulting in possible tensions in decisions towards information disclosure and CTA use, since the information shared is highly private, including health and location tracking data. Additionally, CTAs do not function as discrete artifacts; they are installed on personal devices and with those devices' functionalities and services.

The longitudinal design was chosen as it enabled us to observe the stability of privacy dynamics in the family dyads over time. Our initial data collection was early in the pandemic when information about proper mitigation was less clear, and CTAs were less familiar to the population. Over time, including at the time of the

second data collection, shifting information about the pandemic could influence behaviours related to use of CTAs (e.g. perceiving higher or lower benefits from using the technology).

3.1. Participants

Subjects were recruited via Qualtrics panel services at both Time 1 (T1, September–October 2020) and Time 2 (T2, February–March 2021). This research was approved by the Institutional Review Board at the lead institution prior to data collection. Respondents were from various regions of the US, representing diversity in terms of gender, race, ethnicity, education, occupation, age, and geographic location.⁴ Teenagers had to be between 13 and 17 years old, have a smartphone, and live in the responding parent or guardian's home. The choice of teenagers in this age range ensured they had 'the developmental capacity to make decisions about information sharing' (Hiller et al. 2008). At T1, 379 parent-teen dyads completed the survey. At T2, we received complete responses from 109 of those dyads (after removing dyads with missing data or who failed the attention checks). Most parents were employed at both timepoints (68.8%), with 33% reporting their employment as essential at T1 and T2. The sample had a relatively equal gender distribution (45.9% male parents; 49.5% male teens). Most respondents were Caucasian (76.1% parents; 71.6% teens), and most parents were married at T1 (69.7%) and T2 (67.9%). A wide variety of educational backgrounds and income levels were included.

3.2. Instruments

The instruments (pre and post) included previously used scales, except for concern for family privacy, which was adapted from the concern for privacy construct (Smith, Milberg, and Burke 1996). They were pre-tested, and once refined, they were pilot tested with 71 dyads of student roommates (i.e. living together) at a large public university, augmented with several parent-teen dyads. The design ensured that neither parents nor teens could return through the survey to see each other's answers. Attention check questions were included for data quality purposes. A marker variable was included to account for scale psychometric properties. The instrument required parents to grant permission for their teen to participate and teens to assent electronically. Parents completed the first part of the survey and responded to questions about themselves. They were then asked to have their teenager complete the second portion of the survey.

The survey did not allow the teen to go back and see the parent's responses. After the teen completed their portion of the survey, they were asked to return the survey to the parent, who provided the final submission. Again, the parent could not go back and see the teen's responses. The T1 and T2 instruments used the same question order, and dyads took approximately 30–40 min to complete the surveys at each time point. Items are listed in Appendix A1, and the reliability and validity tests for these items are provided in Appendix A2.

3.3. Dataset preparation

We used SPSS scripts to convert our dataset into a dyad format (Kenny 2006). The distinguishable nature of the members of our dyad required us to utilize a standard dyadic design where each member of a dyad could only be part of one dyad (Kenny, Kashy, and Cook 2006). This resulted in the data collected for each member of the dyad being represented in one record within the dataset. Prior to dataset conversion, each individual of the dyad had their data as separate records. Follow-up tests, including t-tests and descriptive statistics, were calculated in SPSS version 29.0.2.

3.4. Latent profile analysis

We conducted a latent profile analysis to address our research question about which types of dyads are more amenable to disclosing information via technology (Lazarsfeld and Henry 1968; Spurk et al. 2020). This approach identifies latent groups within a dataset using probabilistic configurations of variables (Spurk et al. 2020). A closely related and more common analysis type is latent class analysis (Oberski 2016). The key difference is that latent profile analysis allows for the use of ordinal and continuous data, whereas latent class analysis primarily works with categorical data. As a result, latent profile analysis offers a flexibility well suited to behavioural scholarship, as it can be used with variables measured on Likert scales, for example. In short, the method allows us to identify theoretically interesting subpopulations in our data that aggregation-based analyses would miss (Mattke et al. 2018). Since there is limited use of this approach in the IS literature, and none we could identify for dyadic longitudinal datasets, we draw on the psychology literature for guidance on conducting latent profile analysis on longitudinal dyadic datasets. When conducting a latent profile analysis, multiple classifications of the data are generated.

Selecting the optimal profile solution is informed by both statistical indicators and the researcher's theoretical considerations. We tested our profile solutions with four different measures. The Akaike's Information Criterion (AIC) fit measure (Akaike 1973, 1987) is based on maximum likelihood estimation (MLE), where a lower score indicates a more parsimonious model (Tein, Coxe, and Cham 2013). We also use the Bayesian Information Criterion (BIC), a fit measure (Schwarz 1978) based on MLE and Bayesian analysis; a lower score indicates a more parsimonious model (Tein, Coxe, and Cham 2013). The entropy fit measure (Celeux and Soromenho 1996) evaluates classification uncertainty, with values $> .80$ indicating good fit of the model (Tein, Coxe, and Cham 2013). Lastly, we conducted a Bootstrapped Likelihood Ratio Test (BLRT) (McCutcheon 1987; Peel and McLachlan 2000). For this test, maintaining the null hypothesis means that the model with one less profile is the statistically optimal model. We use multiple profile evaluation metrics rather than just one to ensure that our profile models are statistically robust, especially given the limitation of a smaller sample size. While there are no strict guidelines on sample size, the median sample size for latent profile studies has been found to be 494 (Spurk et al. 2020), which includes mostly non-dyadic non-longitudinal studies.

Selecting the number of profiles is the most nuanced step of the process as it requires theory-informed judgement from the researcher (Spurk et al. 2020). The above tests and metrics represent baselines to establish the statistical validity of the profile solution. However, it is usually the case that there will be multiple profile solutions that pass the thresholds of the tests used (e.g. a two-profile solution and a three-profile solution could both meet the statistical requirements). When a solution is selected the profiles generated are also not attributed any name or context from the classification algorithms.

We used R 4.3.2 with the packages tidyLPA (Rosenberg et al. 2021), dplyr (Wickham et al. 2022), and tidyverse (Wickham and Rstudio 2022) to build and analyze the profiles. Consistent with our conceptualisation of the dyadic privacy calculus as an interdependent configuration of individual perceptions, profiles were constructed using conjoint parent and teen responses in the dyad rather than aggregated or latent higher-order variables. These profiles were constructed using measures of perceived CTA benefits, self-privacy concern, and family privacy concern for both the teen and the parent in each dyad. This list of constructs means that each profile is constructed from six measures. When constructing profiles, we included measures from a single time point, thus estimating profiles separately for T1 and T2 data.

4. Results

To answer our research question regarding how interdependent privacy perceptions influence parent – teen disclosure decisions, we used the latent profile analysis (LPA) to identify groups of dyads characterised by distinct combinations of privacy concerns and perceived benefits. The approach can help capture interdependent privacy perceptions and their effects on disclosure intentions. We used the AIC, BIC, Entropy, and BRLT metrics as a baseline for the quality of the various profile solutions and selected the profile solution that had the most theoretical clarity. We also plot the various profile solutions to help determine which solutions had profiles that could be discriminated from each other and classified into theoretically meaningful labels (Berlin, Williams, and Parra 2014; Spurk et al. 2020). For example, if two profiles in a solution overlap significantly, the overlap may suggest a lack of theoretical clarity and difficulty of discriminating between two profiles. Table 1 summarises the rules for fit indices while Table 2 presents the results of our LPA analyses for T1 data for the different solutions that consider different profile numbers.

4.1. Profile identification

Examining the metrics in Table 2, it became clear that the two-profile solution was desirable because it met

Table 1. Profile evaluation metrics.

Metric	Description
Akaike's Information Criterion (AIC) (Akaike 1973, 1987)	Based on maximum likelihood estimation (MLE); lower score indicates a more parsimonious model (Tein, Coxe, and Cham 2013)
Bayesian Information Criterion (BIC) (Schwarz 1978)	Based on MLE and Bayesian analysis; lower score indicates a more parsimonious model (Tein, Coxe, and Cham 2013)
Bootstrapped Likelihood Ratio Test (BLRT) (McCutcheon 1987; Peel and McLachlan 2000)	Test where maintaining the null hypothesis means the model with one less profile is the statistically optimal model (Tein, Coxe, and Cham 2013)
Entropy (Celeux and Soromenho 1996)	Evaluates classification uncertainty; values > .80 indicate good fit (Tein, Coxe, and Cham 2013)

Table 2. Profile Fit Indices – Time 1.

Profiles	AIC*	BIC*	Entropy*	BRLT*	BRLT <i>p</i>
1	1873.944	1906.240	1.000		
2	1621.634	1672.770	0.931	266.309	0.010
3	1529.297	1599.272	0.921	106.337	0.010
4	1451.472	1540.286	0.961	91.825	0.010
5	1428.368	1536.021	0.921	37.104	0.010

AIC: Akaike's Information Criterion (Lower score is more parsimonious model); BIC: Bayesian Information Criterion (Lower score is more parsimonious model); Entropy (> .80 indicates good model fit); BRLT: Bootstrapped Likelihood Ratio Test (Maintaining null indicates optimal model has one fewer profile).

AIC, BIC, and entropy model-fit thresholds and offered greater theoretical clarity than the other profile solutions (i.e. it is consistent with the privacy calculus model). Some solutions with more profiles also met statistical thresholds but did not offer additional theoretical clarity or differ substantially in structure from the two-profile solutions. The two-profile solution provides theoretical parsimony without sacrificing statistical validity. In profile 1 dyads, both the parents and the teens have high perceived CTA benefits, low self-privacy concern, and low family privacy concern. We label these *technology-receptive* parent-teen dyads. In profile 2 dyads, the parents and teens have lower perceived CTA benefits, higher self-privacy concern, and higher family privacy concern. We label these as *technology-resistant* parent-teen dyads.

Figure 1 plots the two profiles with standardised values for each of the profile variables. The bars represent the 95% confidence interval for each profile variable and the boxes represent one standard deviation within each profile variable (Rosenberg et al. 2021). There is some overlap on individual measures between different profile standard deviations, but the profile classification algorithm makes an assignment based on all the measures. The plotted lines connect the cluster centroids for the respective profile, showing the average point on the specific measure for dyads assigned to the profile.

4.2. Longitudinal stability of profiles

A deeper understanding of our research question can be obtained by examining the longitudinal stability of the dyadic profiles. To better understand the longitudinal perceptions related to the calculus regarding CTA, we conducted the LPA analysis again at T2. The profile fit indices are presented in Table 3. Results show that the two-profile solution remains statistically valid at T2. Therefore, for theoretical consistency over time, we chose the two-profile solution again and found that the two profiles follow the same trends as those at T1. These results, which support the stability of the two-profile solution over time, suggest our profiles are both methodologically and theoretically valid longitudinally. Figure 2 shows a plot of the two-profile solution at T2.

While the relative stability of the two profiles over time suggests that interdependent privacy perceptions are collectively reinforced within families, we did examine the dyads to see which ones shifted to a different profile. We did find a few instances where profiles shifted. Table 4 shows the total number of dyads in each profile, as well as the number of dyads that shifted

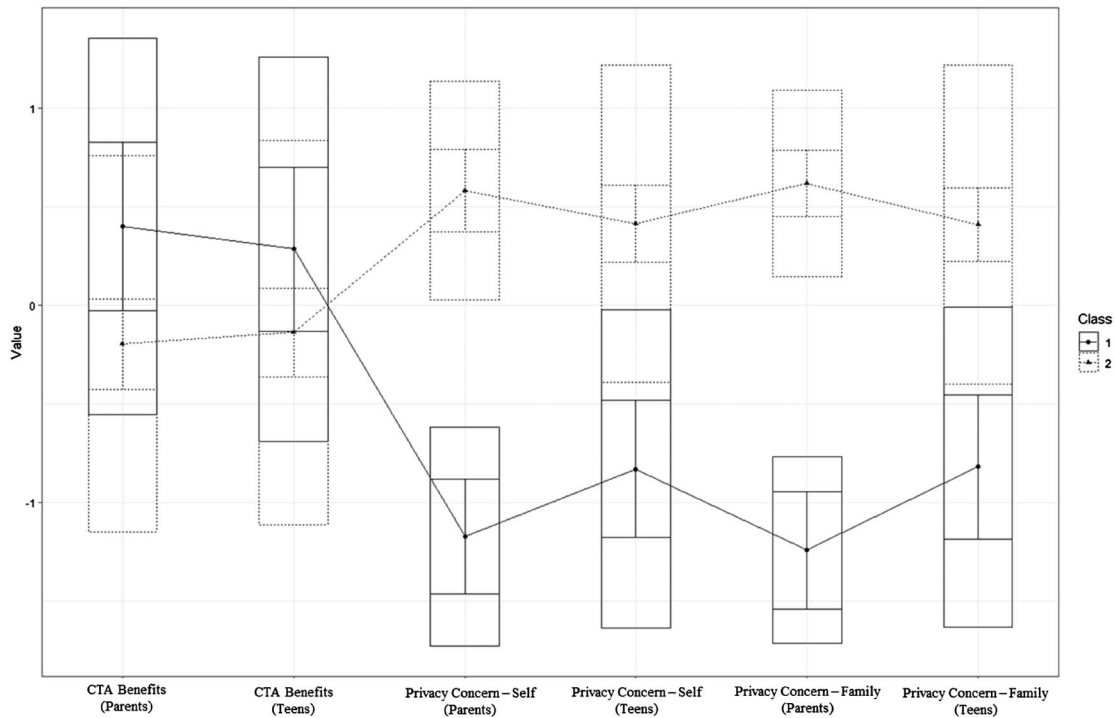


Figure 1. Profile Plot – Time 1.

Table 3. Profile fit indices – time 2.

Profiles	AIC*	BIC*	Entropy*	BRLT*	BRLT <i>p</i>
1	1873.944	1906.240	1.000		
2	1535.237	1586.373	0.968	352.707	0.010
3	1434.347	1504.322	0.972	114.890	0.010
4	1353.806	1442.620	0.983	94.542	0.010
5	1342.429	1450.083	0.935	25.377	0.010

AIC: Akaike's Information Criterion (Lower score is more parsimonious model); BIC: Bayesian Information Criterion (Lower score is more parsimonious model); Entropy (>.80 indicates good model fit); BRLT: Bootstrapped Likelihood Ratio Test (Maintaining null indicates optimal model has one fewer profile).

profiles T1 and T2. In total, 12 profiles shifted from technology-receptive to technology-resistant, and 9 shifted from technology-resistant to technology-receptive.

4.3. Post hoc analysis: intra-dyad variations and alignment

The latent profiles we developed were based on dyadic data (considering conjointly the perceptions of the parent and those of the teen); however, they were constructed based on responses from individuals within the dyads. This structure gives us the ability to investigate for potential variations and/or alignment between parents and teens in our profiles. To examine these, we conducted two-tailed paired sample t-tests between parents and teens within each profile assignment at T1 and again at T2 using the variables that helped in profile development. Additionally, we tested for

differences in intention to use CTA between the two types of respondents in each profile. Results are reported in Tables 5 and 6.

We observe that in the technology-receptive profile, teens were significantly more concerned about self-privacy and family privacy than parents at T1 and T2. For the technology-resistant profile, teens saw significantly more benefit to CTAs, and parents had higher family privacy concerns at T1. At T2, in the technology-resistant profile, teens were significantly more concerned about self-privacy and family privacy. Despite differences between parents and teens, they are more aligned with each other than with the dyads in the opposite profile. For example, at T1 both profiles show differences in family privacy concern between the parents and teens in the dyads. However, in the technology-receptive profile, parents had a mean of 1.676 and teens a mean of 2.439 for family privacy concerns, whereas in the technology-resistant profile, parents had a mean of 4.379 and teens a mean of 4.042. It is both true that dyads are largely aligned, and yet family members of the dyad may still have different perceptions on the margin.

4.4. Post hoc analysis: behavioural correlates of dyadic privacy profiles

We conducted a second set of post-hoc analyses to determine whether the profiles would apply to additional related behaviours beyond technology

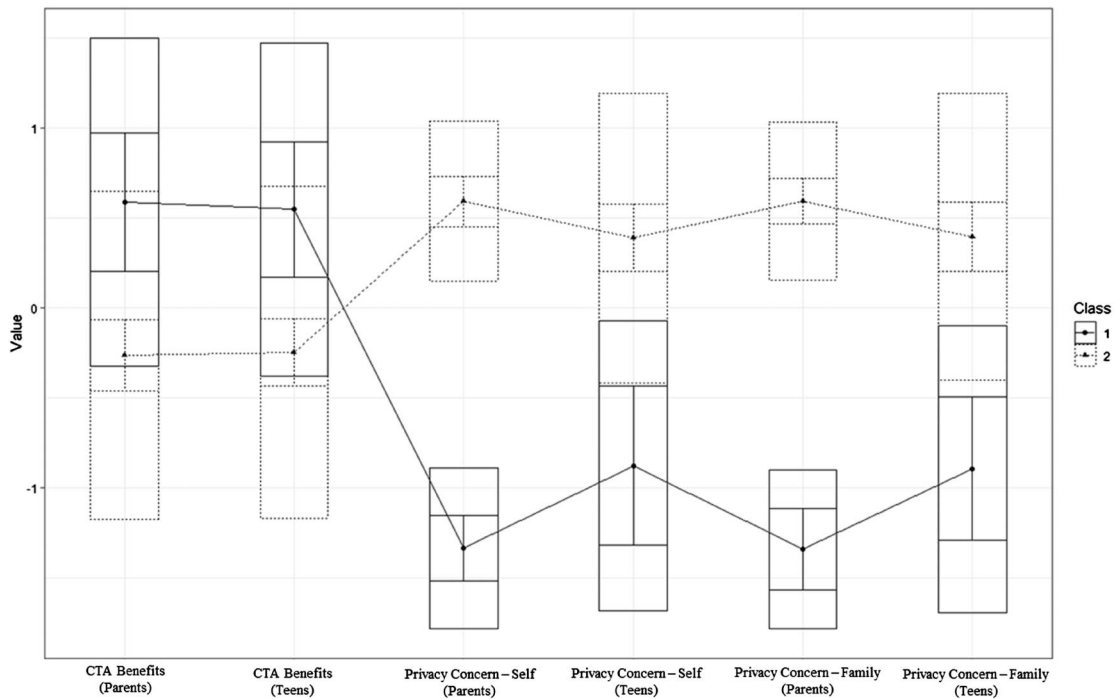


Figure 2. Profile Plot – Time 2.

Table 4. Profile membership.

Profile	Label	Time 1	Time 2	Shifted 1 – > 2	Shifted 2 – > 1
Profile 1	Technology receptive	37	34	12	9
Profile 2	Technology resistant	72	75		

choices that require information disclosure. Our study utilised profile analysis to develop two distinct dyadic profiles based on the privacy calculus model: technology-receptive and technology-resistant dyads. These profiles are useful for identifying distinct groups in a dataset, but they can also be used to measure differences between these groups on different outcomes. The privacy calculus was initially developed (Culnan and Armstrong 1999) by leveraging the broader calculus of

behaviour (Laufer and Wolfe 1977). Therefore, in this post-hoc analysis, we investigate whether our profiles would hold in terms of CTA use intentions and other behaviours related to contact tracing (i.e. behaviours related to health guidelines) using additional data on these behaviours. We test differences in reported behaviours by dyads of parents and teens from each profile (technology-receptive and technology-resistant) at each time point using one-tailed t-tests (see Table 7 for T1 and Table 8 for T2). One-tailed tests are utilised because we expected the differences based on our profile analysis would also apply to related safety guidelines.

Profiles generated in R were coded with dummy variables and imported into SPSS. We conducted Levene's test to determine whether equal variances could be assumed when calculating the t-statistics. Since t-tests

Table 5. Parent-teen differences – time 1.

Behaviour	Profile 1 – Technology Receptive				
	Mean P	Mean T	t(df)	p-value	Cohen's d
CTA Benefits	3.350	3.430	−0.199 (36)	0.843	2.476
Privacy Concern – Self	1.662	2.324	−3.330 (36)	0.002	1.209
Privacy Concern – Family	1.676	2.439	−4.231 (36)	<.001	1.098
Intention to Use CTA	3.050	2.780	1.281 (36)	0.208	1.283
Behaviour	Mean P	Mean T	t(df)	p-value	Cohen's d
CTA Benefits	1.690	2.210	−2.150 (71)	0.006	2.028
Privacy Concern – Self	4.194	4.014	1.273 (71)	0.104	1.204
Privacy Concern – Family	4.379	4.042	2.847 (71)	0.035	1.004
Intention to Use CTA	2.390	2.140	1.810 (71)	0.074	1.172

P: Parent; T: Teen.

Bold values indicate a p-value of less than 0.05.

Table 6. Parent-teen differences – time 2.

Profile 1 – Technology Receptive					
Behaviour	Mean P	Mean T	t(df)	p-value	Cohen's <i>d</i>
CTA Benefits	3.740	3.760	−0.075 (33)	0.941	2.289
Privacy Concern – Self	1.3676	2.206	−3.844 (33)	<.001	1.272
Privacy Concern – Family	1.515	2.110	−2.731 (33)	0.010	1.272
Intention to Use CTA	3.210	3.000	0.942 (33)	0.353	1.274
Profile 2 – Technology Resistant					
Behaviour	Mean P	Mean T	t(df)	p-value	Cohen's <i>d</i>
CTA Benefits	1.510	1.570	−0.331 (74)	0.741	1.742
Privacy Concern – Self	4.253	3.943	2.436 (74)	0.017	1.102
Privacy Concern – Family	4.413	3.913	1.768 (74)	<.001	0.987
Intention to Use CTA	2.150	1.970	1.327 (74)	0.189	1.132

P: Parent; T: Teen.

Bold values indicate a *p*-value of less than 0.05.

Table 7. Mitigation behaviours – time 1.

Parents					
Behaviour	Mean P1	Mean P2	t(df)	p-value	Cohen's <i>d</i>
Intention to Use CTA	3.054	2.389	2.437 (81.117)	0.009	0.474
Avoid gatherings	4.541	3.875	3.548 (106.560)	<.001	0.601
Stay home	4.054	3.639	1.768 (93.548)	0.040	0.325
Social distance	4.405	4.361	0.229 (107)	0.410	0.046
Teens					
Behaviour	Mean P1	Mean P2	t(df)	p-value	Cohen's <i>d</i>
Intention to Use CTA	2.784	2.139	2.400 (107)	0.009	0.485
Avoid gatherings	4.000	3.964	1.416 (93.522)	0.080	0.260
Stay home	3.973	3.583	1.804 (95.716)	0.037	0.329
Social distance	4.189	4.111	0.379 (107)	0.353	0.077

P1: Profile 1 (guideline-receptive); P2: Profile 2 (guideline-resistant).

Bold values indicate a *p*-value of less than 0.05.

Table 8. Mitigation behaviours – time 2.

Parents					
Behaviour	Mean P1	Mean P2	t(df)	p-value	Cohen's <i>d</i>
Intention to Use CTA	3.206	2.147	3.632 (107)	<.001	0.751
Avoid gatherings	4.706	3.867	4.833 (106.830)	<.001	0.780
Stay home	4.412	3.493	4.581 (105.679)	<.001	0.753
Social distance	4.647	4.253	2.409 (96.693)	0.009	0.420
Teens					
Behaviour	Mean P1	Mean P2	t(df)	p-value	Cohen's <i>d</i>
Intention to Use CTA	3.000	1.973	3.895 (107)	<.001	0.805
Avoid gatherings	4.588	3.853	3.994 (106.906)	<.001	0.643
Stay home	4.118	3.533	2.608 (77.180)	0.005	0.500
Social distance	4.294	4.067	1.086 (107)	0.140	0.225

P1: Profile 1 (guideline-receptive); P2: Profile 2 (guideline-resistant).

Bold values indicate a *p*-value of less than 0.05.

assume equal variances, in cases where the Levene's test hypothesis is rejected, we use the adjusted *t*-statistic and degrees of freedom values when reporting our results (Tables 6 and 7). Because the profiles are no longer limited to technology, we refer to these as *guideline-receptive* and *guideline-resistant* dyads in these analyses. We also note that we conducted the analyses by using profiles (dyadic perceptions) to then test their effects on reported behaviours by parents and teens individually, providing a set of cross-level effect tests.

The results indicate differences in the reported behaviours by the profiles for both parents and teens at T1,

which become more pronounced at T2. This difference is evident through larger effect sizes and more behavioural outcomes being significantly different across profiles at T2. At T1, the environmental context was of high risks, high uncertainty, and substantial fear. At T2, more was known about the high risks, but individuals were more accustomed to how to behave during the pandemic, and importantly, there was a glimmer of hope for vaccines.

The intention to use CTA remained consistent across both time points, indicating that profile assignment based on privacy characteristics is a strong predictor

of intentions to use a privacy-invasive, but useful, technology such as CTA. At T1, teens and parents in the guideline-receptive profile were also more receptive to the idea of staying home, while parents were also more receptive to the concept of avoiding gatherings. Social distancing was equally strong between profiles for both parents and teens. This finding likely reflects the strong message in the media about the importance of social distancing to avoid contracting the disease. At T2, teens and parents in the guideline-receptive profiles were more likely to use all related behaviours (avoid gatherings, stay home, social distancing) than those in the guideline-resistant dyads except for social distancing for teens.

These results extend our understanding of interdependent privacy by showing that dyadic privacy orientations also predict related behavioural intentions, consistent with the privacy calculus model. The results also indicate the importance of the environmental context in a privacy or protective measure decision and the capability of profile analysis to enhance understanding of decisions involving related family members.

5. Discussion

We report on our research that seeks to explore how the interdependent privacy perceptions of parents and teens influence their information disclosure decisions via technology usage. To conduct the research, we created profiles of family dyads based on their privacy perceptions regarding intentions to use CTAs. A latent profile analysis at two points in time allowed us to develop a deeper understanding of the nuances of how family characteristics affect decisions than would have been possible with aggregated results. By collecting data at two different points in time from these dyads, we better understand collective-level privacy decisions over time. The findings demonstrate that information disclosure decisions within families are shaped by shared, interdependent privacy perceptions rather than by individual evaluations alone. By identifying two distinct dyadic profiles – technology-receptive and technology-resistant – the empirical analyses reveal that parents and teens tend to form stable, collective privacy orientations (of the risks and benefits) that shape their shared intentions to disclose information via technologies (CTAs in this study), even when individual family members differ in the strength of their concerns. Across time, these dyadic patterns remain largely consistent, indicating enduring collective privacy norms that guide technology-related decisions within families. We provide empirical support for the joint effect of parent and teen privacy perceptions on their

disclosure decisions, addressing the research question by showing that interdependent privacy beliefs predict consistent and coordinated technology use within families. The results highlight the importance of viewing privacy decision-making as a collective process, shaped by relational influence and shared perceptions, rather than solely as an individual calculus.

5.1. Theoretical interpretation of dyadic privacy profiles

Although the latent profiles identified in this study are empirically derived from privacy calculus variables, they should not be interpreted as mere aggregations of individual perceptions. These profiles should not be interpreted as representing a higher-level dyadic privacy construct. Instead, they reflect stable configurations of interdependent individual perceptions that emerge through relational processes within the parent-teen dyads. As such, we theorise these profiles as relational orientations toward collective privacy that emerge from repeated interaction and mutual influence within a parent-teen dyad. This interpretation aligns with multilevel perspectives on privacy, which emphasise that privacy decision-making is embedded within social structures and relationships (Bélanger and James 2020). In dyadic relationships characterised by nonindependence (Kenny, Kashy, and Cook 2006), individual privacy perceptions are likely not formed or enacted in isolation but are shaped by shared familial histories, expectations, negotiations, and power relations embedded in the parent-teen relationship. The technology-receptive and technology-resistant profiles reflect qualitatively different ways in which dyads collectively interpret and manage privacy risks and benefits, rather than simply differing levels of concern or perceived utility. From this perspective, the profiles identified through latent profile analysis represent relational states or configurations of shared and partially shared perceptions that guide coordinated disclosure intentions.

With this theoretical interpretation in mind, in technology-receptive dyads, both parents and teens perceive substantial benefits from technology use while expressing comparatively lower concerns about privacy risks to themselves and their family. Prior research on family systems emphasises that families, across the generations, develop patterned ways of coordinating behaviour and managing uncertainty over time (Allen and Henderson 2023; Daly 2003). Technology-receptive dyads may thus reflect families in which such coordination has extended to privacy and technology-related domains. Importantly, this orientation does not imply the absence of concern or conflict. Rather, it suggests that concerns

can be managed within a relational framework that allows the dyad to reach coordinated decisions. The presence of intra-dyad differences within this profile – such as teens reporting higher privacy concerns than parents – can be interpreted as evidence of negotiated alignment rather than discord. Consistent with communication privacy management theory (Petronio 2013), these dyads appear to have developed implicit or explicit rules governing acceptable disclosure, enabling collective action despite differences in individual preferences.

For technology-resistant dyads, perceived benefits are lower and privacy concerns are greater at both the individual and family levels, suggesting that the collective stance toward disclosure is shaped more by perceived risks than by anticipated gains. Family research highlights that parent – teen relationships are often marked by power asymmetries, particularly around issues of autonomy and protection (Ogolsky, Whittaker, and Monk 2019; Steinberg 2014). From this perspective, resistance does not simply reflect ‘low adoption propensity,’ but rather a relational dynamic in which concerns about privacy, control, and potential harm dominate collective decision-making, and in most families, the concern could be top-down (from the parent to the teen). Heightened parental concern for family privacy, coupled with teens’ own privacy concerns, may signal a lack of shared understanding regarding the purpose, scope, or consequences of technology use, or may even mask the parents’ greater power in the relationship to exert more control over the family’s access to the outside world.

The presence of systematic differences between parents and teens within each profile is theoretically informative rather than problematic. Instead of undermining the coherence of the profiles, these differences suggest that dyadic privacy orientations emerge through processes of negotiation and influence, consistent with theories of family interaction as a dynamic process and multilevel privacy management (Bélanger and James 2020; Daly 2003). Even when parents and teens differ in the intensity of their privacy concerns or benefit perceptions, they may still arrive at coordinated intentions that distinguish them from other dyads. This pattern reinforces the interpretation of the profiles as collective outcomes rather than uniform individual states. In this sense, the profiles capture aligned outcomes of interaction, not perfect agreement. The finding that dyads are more similar within a profile than across profiles supports the idea that relational influence shapes privacy decision-making in systematic ways. Such alignment amid difference is consistent with prior work on dyadic and family decision-making,

which shows that coordination often emerges despite ongoing disagreement (Allen and Henderson 2023; Kenny, Kashy, and Cook 2006). Families are interactional units, charged by society at large with the structural roles in which parents are responsible for developmentally helping their children become acceptable members of the parents’ own society. The latent profiles reflect stable relational orientations that accommodate individual variation while producing coherent collective stances toward disclosure.

Taken together, these interpretations position the latent profiles as snapshots of ongoing social processes rather than static attitudinal clusters. Privacy calculus evaluations do not occur in a vacuum; they are shaped by repeated interaction, shared experiences, and evolving contextual cues (Bélanger and James 2020; Laufer and Wolfe 1977). Over time, families may develop relatively stable orientations toward privacy and technology use that guide behaviour across situations, even as specific risks and benefits change. The observed longitudinal stability of the profiles supports this interpretation, suggesting that these relational orientations function as enduring family-level norms rather than momentary responses to a specific technology. We emphasise that these theoretical interpretations are necessarily provisional, given the exploratory nature of the study. However, making the relational dynamics underlying the profiles explicit advances theory by moving latent profile analysis beyond descriptive categorisation toward theoretically meaningful constructs. By interpreting profiles as emergent relational states shaped by trust, power, communication, and coordination, this study contributes to a deeper understanding of collective privacy decision-making and demonstrates how empirically derived profiles can be integrated with established theories of family dynamics and multilevel privacy management.

5.2. Advancing collective information privacy and extending the privacy calculus

This study explores the information-sharing decisions of a unique collective, the family, by consolidating the perceptions of a dyad’s members into a collective perception. The research helps expand the conceptualization of privacy decision-making beyond the individual and empirically grounds privacy as a collective, dyadic process. The family offers an excellent unit in order to understand how the privacy calculus is navigated by two diverse individuals, because of the hierarchy of roles inherent in the parent-teen dyad. While prior research has highlighted interdependent privacy concerns, most studies continue to measure

privacy calculus at the individual level. Our findings show that parents and teens develop shared perceptions of benefits and privacy concerns that combine to produce distinct dyadic privacy orientations, illustrating that individual perceptions are systematically shaped by relational influence and shared contextual experiences. Importantly, disclosure intentions align with these dyadic privacy profiles, demonstrating that information disclosure is coordinated at the collective level even when subtle intra-dyadic differences exist. Technology-receptive dyads, or those who see high benefits and fewer privacy concerns, are more likely to use CTAs, even if they perceive these as requiring the sharing of personal information. The opposite is true for technology-resistant dyads, who perceive lower benefits and greater privacy concerns, and are less likely to use CTAs. Prior work measured individual perceptions, and to some degree information and interaction management via one person's decision about what to share and whom to share with (i.e. an individual's perceptions) (Laufer and Wolfe 1977), but our findings extend these via dyadic analyses. Our work supports the need to study the under-researched area of collective privacy (Bélanger and James 2020).

By showing that the privacy calculus can operate as a dyadic-level phenomenon, this study extends the privacy calculus framework to account for collective perceptions, collective concerns, and relationally coordinated decisions. Even when family members' perceptions differ, their decisions may still align, creating a collective perception that sets them apart from other collectives, at least when considering the costs and benefits of using technology that requires information sharing. Family interpersonal dynamics require further study to see if they apply to other technology-enabled environments. Of interest is how power dynamics play out with members of the same generation, compared to our examination of intergenerational relationships.

Our work suggests extending the privacy calculus to consider the privacy concerns of other family members. In the family environment, the risks and benefits of sharing information with the use of technologies that may reveal family members' information suggests that families may rely on a combination of general social norms that dictate how families should interact (Johnson, Mollborn, and Horne 2025) as well as their own unique style of interpersonal relating and emotional expression (Daly 2003) regarding the family's information-sharing behaviour and other behaviours, including how to adapt to a major crisis (such as a pandemic). More research is needed to uncover the factors that drive this possible conceptualisation of families, a study that requires examining the intersection of

information systems and family science (Allen et al. 2025). Future work should also consider the competing perspectives of the individuals who comprise the collective. Parents and teens have a shared identity, and at the same time, the adolescent is working to forge a unique identity (Steinberg 2014). If this context were social media usage and sharing of information in a more hedonic context, would there be less alignment between parents and teens?

5.3. Demonstrating stability and temporal structure of collective information privacy processes

Overall, there is limited research on how privacy evolves over time, aside from theoretical models proposing that information privacy decisions involve feedback loops (Bélanger and James 2020; Laufer and Wolfe 1977). Our findings provide longitudinal evidence that suggests the dyadic privacy profiles identified at T1 persist at T2, suggesting that collective privacy perceptions are relatively stable over time. However, a small number of dyads shift between profile categories. When this happens, they align with expected interpretations of the evolving pandemic context. These findings suggest that collective privacy orientations might function as enduring family-level norms, reinforcing the idea that privacy calculus processes are shaped by lasting social structures rather than only momentary individual appraisals. These insights would not have been unearthed with traditional aggregated analyses. An additional insight comes from the consistent predictive power of the profiles on other related behaviours (i.e. adherence to other pandemic guidelines). This provides further empirical evidence that collective privacy perceptions influence broader behavioural patterns across time. These findings also reinforce the importance of the environmental context in understanding calculus of behaviour (Laufer and Wolfe 1977). This consistency over time, both within and across dyads, could extend to the rest of the family, which needs to be examined in future research. Should future research continue to support consistency over time it would lend credence to an important theoretical insight, that measuring calculus-based perceptions at a single time point is likely influenced by the context in which they are measured. Time would then most likely promote the possibility that family members learn from each other and develop some norms of receptiveness or resistance to guidelines (in our context). Together, these findings would extend theoretical models of privacy by demonstrating that privacy perceptions and their associated behaviours are temporally durable within collectives.

Our post-hoc analyses were exploratory, so any insights require rigorous validation in future research. Nevertheless, the relative consistency of perceptions over time, as revealed in our post-hoc analyses examining both within and across dyad changes, suggests that family members influence each other in their perceptions and decisions, even if their decisions ultimately remain individual. Figure 3 illustrates a possible process by which dyadic perceptions can lead to decisions that may be reinforced or challenged over time, and how they may fit within the broader family context. It is possible that this process develops an accepted way of handling situations in the family, which needs further study.

Consistent with the MDTP and other theoretical lenses, Figure 3 suggests that the environment or context affects individual perceptions. However, the environment also affects individuals within collectives, in our study dyads. Those who are receptive in this context (i.e. sharing information via an app during COVID in our study) are more likely to see the benefits of the technology as higher than those who are resistant. In a collective, such as the family, however, each member of the collective can influence the ultimate decision of the family, particularly as children age and are able to engage with their parents. However, it is through time, when families or dyads discuss the resulting effects or through observations of those effects, that collectives may develop enough similarities to establish norms of behaviour that will affect perceptions in future similar situations. This exploratory insight could be further examined through an extensive longitudinal

study design that aims to understand the process of influence within the collective. A longitudinal study that measured actual behaviours could also help explain the few profiles that did change over time. Perhaps these families were ones that were living within a privacy paradoxical situation where their information privacy concerns were not consistent with their behaviours, and as this inconsistency was recognised, either their concerns or their intentions changed to better align with their behaviours.

5.4. Leveraging profile analysis for multilevel studies

Our research illustrates the value of latent profile analysis as a methodological tool for studying collective privacy decision-making. This approach recognises individual perspectives by not aggregating dyadic metrics, while also acknowledging the collective through dyadic-level profile assignments. It can be utilised for further investigation into whether our findings about dyads extend to the entire family. Our dyad comprised a parent and a teen in a unique power dynamic. When more family members are included and power dynamics change, would similar results hold, or would there be more differences within families, or more convergence and solidarity? A profile analysis can be used to study such other collectives in different settings. Our research illustrates how future research can investigate privacy decision-making not only within families. For example, information disclosure decisions within a workgroup could be investigated using dyadic

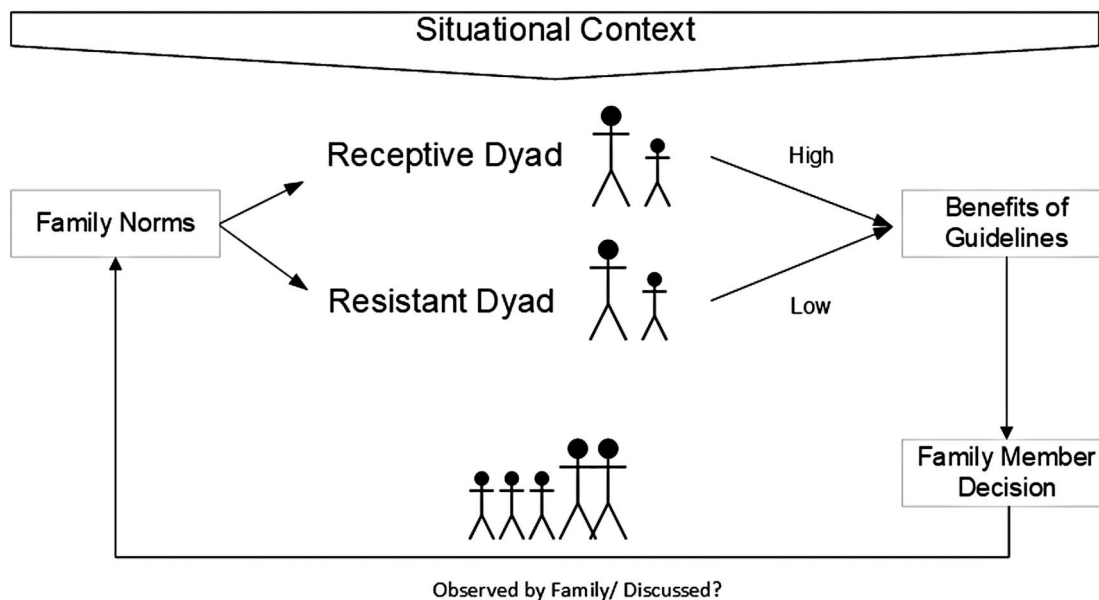


Figure 3. Proposed Importance of Context in Calculus of Behaviour Research.

responses from a worker and their supervisor, given the differential power dynamics that exist in organizations. Another dyad of interest could be romantic partners or spouses. Is there something about parents and teens (an intergenerational pairing) that would replicate to intra-generational pairs of intimate partners? There is an abundance of literature on power differentials in relationships, particularly in terms of how people with less power have more insight into people with more power than vice versa (Ogolsky, Whittaker, and Monk 2019), and this literature may help inform collective technology decision-making.

In addition to studying other dyadic relationships, profile analysis could be applied to contexts with more than two people, such as an entire family. This approach can be scaled in two ways. One way is to include measures for each family member, as we did for parents and teens in our construction of dyadic profiles. The complication with this approach is that as each additional family member is added, the measures used to build the profile must be duplicated (e.g. three measures for two parents and a child is nine total measures for profile construction). Another approach is to average the responses of family members into a single measure and build profiles using the aggregate scores instead of the individual scores. A hybrid approach could aggregate by groups, such as adults and children in a household. Which approach is best will depend on the context of the research. If individual granularity is important, the aggregation approach may not be a good fit, but if the focus is solely on the family unit, aggregated profiles may be preferable. In addition, dyadic analysis could be used with a variety of theoretical lenses, studying other perceptions that may affect a collective, such as knowledge and self-efficacy, and, other constructs that reflect collective-level dynamics, including power, cohesion, and norms.

While the use of latent profile analysis itself is not new (Lazarsfeld and Henry 1968; Spurk et al. 2020), its application in information systems research is limited. We specifically adapted our analysis from the psychology literature on dyadic longitudinal profile analysis (Roberson et al. 2020). LPA allowed us to identify meaningful dyadic configurations by modelling parent and teen perceptions jointly, preserving individual differences while generating theoretically grounded collective profiles. Since the use of dyadic profiles allows for identifying theoretically interesting individual and collective interactions lost with typical aggregated analysis (Mattke et al. 2018), the approach can help guide future scholarship within information privacy and other domains where interest in dyadic or collective level research is growing (e.g. for spouses, employee-

manager, and other information-sharing dyads). As information sharing decisions are made in other collective-related contexts, we would expect to see different profile structures emerge. Overall, by showing how LPA can be applied to longitudinal dyadic privacy data, we provide a methodological template for future privacy research seeking to uncover multilevel or collective decision patterns that traditional approaches overlook.

Appendix C provides a summary of the contributions in this study. These contributions provide a cohesive theoretical narrative regarding how privacy decision-making within the parent-teen family relationship reflects a collective process shaped by shared evaluations of risks and benefits, reinforced over time, and empirically identifiable through latent profile analysis. Using latent profile analysis enabled us to identify theoretically nuanced subpopulations that would be lost in a traditional aggregation-based analysis, and it is well suited to the complex context of collective privacy decisions. By addressing the research question directly, the study shows that interdependent privacy perceptions of parents and teens are central drivers of their dyadic information disclosure decisions. This work, therefore, lays a foundation for future research to more fully conceptualise and investigate privacy as a multilevel, relational, and collective phenomenon.

5.5. Practical implications

In addition to the theoretical contributions of this work, our results provide insights for practice. Through our analysis we identified different types of parent-teen dyads. Some of these dyads were receptive to privacy-invasive technology while others were resistant. Our findings suggest that organisations and governments cannot take a uniform approach to implementing technology with privacy-invasive components. Increasing perceived benefits and reducing privacy concerns remains critical to influence intention to use these technologies, but what resonates with potential groups of users may differ, and a one-size-fits-all approach may result in lower adoption rates overall. Developers of these technologies may gain insights by directly engaging with technology-resistant groups and testing different approaches to persuade potential users.

Our research also highlights the importance of relationship interdependence in privacy decision making (Zhang and Zhu 2025). While we observe differences between parents and teens within the dyads, they are overall much more aligned than their counterparts in the other profile dyads. From a practice perspective, it is important to understand the surrounding social

relationships of a potential user of a privacy-invasive technology. This is relevant to who a potential user may consider when making a privacy decision, and it could also indicate influence pressures within a social unit. If, for example, an organisation can convince a parent of the benefits of a CTA, the parent might further convince their teen of the value of adopting the technology, bringing them into alignment.

5.6. Limitations and additional research recommendations

Our exploratory research has limitations, which open additional avenues for future research. We only measured dyadic data from a parent and a teen within each family, so we cannot make claims of generalizability to all collectives, not to families in general. Future research could also examine other dyads in the family to see if their profiles are consistent with the family profiles we found in this research. Research could be conducted on all members of a family as opposed to dyads only. Future research should explore profiles in other collective settings with people in various positions of perceived power. While challenging, we also recommend that future research at more than one level to capture the multi-level interactions between individuals of the collective, understanding the individual, dyadic, whole group, and even community levels in which privacy decisions are situated. This research also had a small sample size for conducting a latent profiles analysis. While we used multiple profile evaluation metrics rather than just one to ensure that our profile models are statistically robust, future research could increase the sample size to ensure the models hold without the need of utilising multiples profile evaluation metrics.

Due to our surveys being conducted online we could not verify whether the teen was the one who completed the survey or if the parents did so. However, due to the differences in responses, we are confident that responses were provided by different individuals. Another limitation is the possibility of common method bias (Podsakoff et al. 2003; 2024) introducing variance attributed to the method used rather than the actual target phenomenon of the study. Online surveys such as the Qualtrics panel we used also bring a risk of insincere responses from our participants (Kennedy et al. 2022). Future research could validate our results using methodologies that allow observation of people while they respond. Our study was conducted from 2020 to 2021 and while this was a season of drastic change, the technology used was specific to the time. We anticipate that these results will hold in other situations of interdependent privacy, such as the use of smart home speakers,

smart cars, and shared online subscriptions. As technology advances, it will be necessary to better understand the components that make up a profile and their influence on technology use behaviours.

6. Conclusion

The goal of this study was to examine how two family members' interdependent privacy perceptions affect their information disclosure decisions through technology use. To answer our research question, we thus studied dyads composed of one parent and one teen from the same family. Using latent profile analysis, we identified two distinct types of parent-teen dyads in their approach to information disclosure and technology use: technology-receptive and technology-resistant. Technology-receptive dyads perceived higher benefits and lower privacy concerns regarding the use of contact tracing apps, while technology-resistant dyads showed the opposite pattern. These profiles remained relatively stable over time, indicating that dyadic privacy perceptions are consistent even as external contexts evolve and suggesting that family members influence one another's technology-related intentions in predictable, enduring ways. We then reconceptualize empirically derived privacy profiles as relational orientations toward collective privacy, demonstrating how latent profiles can be theoretically interpreted as outcomes of ongoing social and relational processes within dyads. Post-hoc analyses revealed that technology-receptive dyads were also more likely to engage in other guideline-compliant behaviours during the pandemic, such as staying home or avoiding gatherings, demonstrating that privacy-related perceptions extend to broader behavioural patterns. The latent profile analysis enabled this deeper understanding of collective privacy by identifying these subpopulations lost in traditional aggregation approaches. Overall, the findings support the existence of collective-level privacy decision-making processes that align with the privacy calculus, providing a new understanding of the information-sharing decisions made by collectives. As information privacy research advances, categorising families into distinct groups, such as technology-resistant and technology-receptive, could provide a foundation for further exploring decisions surrounding privacy in various groups.

Notes

1. <https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breach-examples/>
2. <https://www.cm-alliance.com/cybersecurity-blog/digital-privacy-risks-during-family-breakdowns>

3. <https://www.americanbar.org/advocacy/global-programs/news/2024/importance-digital-privacy-emerging-technology/>
4. Compensation was provided by Qualtrics, and the exact payment to participants is unknown to the research team. 109 dyads of parent-teen pairs were surveyed at T1, and the same dyads were surveyed again at T2. The researchers paid Qualtrics \$42.00 for responses that completed surveys at both T1 and T2.
5. <https://www.who.int/emergencies/diseases/novel-coronavirus-2019/advice-for-public>

Acknowledgements

The authors wish to thank the Institute for Society Culture and the Environment at Virginia Tech for comments on an earlier version of this paper.

Author contributions

CRediT: **Robert E. Crossler**: Conceptualization, Data curation, Funding acquisition, Investigation, Methodology, Project administration, Supervision, Writing – original draft, Writing – review & editing; **France Bélanger**: Conceptualization, Data curation, Funding acquisition, Investigation, Methodology, Project administration, Supervision, Visualization, Writing – original draft, Writing – review & editing; **Katherine R. Allen**: Conceptualization, Funding acquisition, Investigation, Methodology, Project administration, Supervision, Writing – original draft, Writing – review & editing; **Julia Stachofsky**: Data curation, Formal analysis, Methodology, Software, Validation, Visualization, Writing – original draft, Writing – review & editing.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This research was funded by the National Science Foundation, Science and Trustworthy Cyberspace (SaTC) [Grant No. SES-2039172, 2020-2021].

ORCID

Robert E. Crossler  <http://orcid.org/0000-0002-8179-9138>

France Bélanger  <http://orcid.org/0000-0002-3213-2636>

Katherine R. Allen  <http://orcid.org/0000-0001-9920-0333>

Julia Stachofsky  <http://orcid.org/0000-0002-5989-821X>

References

- Akaike, H. 1973. “Maximum Likelihood Identification of Gaussian Autoregressive Moving Average Models.” *Biometrika* 60 (2): 255. <https://doi.org/10.1093/biomet/60.2.255>.
- Akaike, H. 1987. “Factor Analysis and AIC.” *Psychometrika* 52 (3): 317. <https://doi.org/10.1007/BF02294359>.
- Allen, K. R., R. E. Crossler, F. Bélanger, J. Resor, and H. A. Kissel. 2025. “Parent and Adolescent Perspectives on Family Problems during the COVID-19 Pandemic: Implications for Family Resilience.” *Family Relations* 74 (1): 7–25. <https://doi.org/10.1111/fare.13105>.
- Allen, K. R., and A. C. Henderson. 2023. *Family Theories Today: A Critical Intersectional Approach*. 2nd ed. Solana Beach, CA: Cognella Academic Publishers.
- ARICI, H. Y. 2021. “The Functionality of Privacy Value in the Continuity of Family Unity.” *Journal of Philosophy, Culture and Religion* 53:44–57.
- Bélanger, F., M. Cefaratti, T. Carte, and S. Markham. 2014. “Multilevel Research in Information Systems: Concepts, Strategies, Problems, and Pitfalls.” *Journal of the Association for Information Systems* 15 (9): 614–650. <https://doi.org/10.17705/1jais.00371>.
- Bélanger, F., and R. E. Crossler. 2011. “Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems1.” *MIS Quarterly* 35 (4): 1017–1041. <https://doi.org/10.2307/41409971>.
- Bélanger, F., R. E. Crossler, K. R. Allen, J. Resor, H. A. Kissel, and T. Finch. 2022. “Family Tensions and Information Privacy: A Barrier to Diffusion of Proximity Tracing Applications?” *Proceedings of the 55th Hawaii International Conference on System Sciences*.
- Bélanger, F., R. E. Crossler, and J. Correia. 2021. “Privacy Maintenance in Self-digitization.” *ACM SIGMIS Database: The DATABASE for Advances in Information Systems* 52 (2): 7–24. <https://doi.org/10.1145/3462766.3462769>.
- Bélanger, F., and T. L. James. 2020. “A Theory of Multilevel Information Privacy Management for the Digital Era.” *Information Systems Research* 31 (2): 510–536. <https://doi.org/10.1287/isre.2019.0900>.
- Berlin, K. S., N. A. Williams, and G. R. Parra. 2014. “An Introduction to Latent Variable Mixture Modeling (Part 1): Overview and Cross-Sectional Latent Class and Latent Profile Analyses.” *Journal of Pediatric Psychology* 39 (2): 174–187. <https://doi.org/10.1093/jpepsy/jst084>.
- Burton-Jones, A., and M. J. Gallivan. 2007. “Toward a Deeper Understanding of System Usage in Organizations: A Multilevel Perspective1.” *MIS Quarterly* 31 (4): 657–679. <https://doi.org/10.2307/25148815>.
- Celex, G., and G. Soromenho. 1996. “An Entropy Criterion for Assessing the Number of Clusters in a Mixture Model.” *Journal of Classification* 13 (2): 195–212. <https://doi.org/10.1007/BF01246098>.
- Chan, E. Y., and N. U. Saqib. 2021. “Privacy Concerns Can Explain Unwillingness to Download and use Contact Tracing Apps When COVID-19 Concerns Are High.” *Computers in Human Behavior* 119:106718. <https://doi.org/10.1016/j.chb.2021.106718>.
- Culnan, M. J., and P. K. Armstrong. 1999. “Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation.” *Organization Science* 10 (1): 104–115. <https://doi.org/10.1287/orsc.10.1.104>.
- Daly, K. 2003. “Family Theory versus the Theories Families Live by.” *Journal of Marriage and Family* 65 (4): 771–784. <https://doi.org/10.1111/j.1741-3737.2003.00771.x>.
- Dienlin, T. 2023. “Privacy Calculus: Theory, Studies, and New Perspectives.” In *The Routledge Handbook of Privacy and Social Media*, edited by Trepte, S. and Masur, P., 70–79. New York: Routledge.

- Dinev, T., and P. Hart. 2006. “An Extended Privacy Calculus Model for E-Commerce Transactions.” *Information Systems Research* 17 (1): 61–80.
- Duncan, S., B. G. Kanki, H. Mokros, and D. W. Fiske. 1984. “Pseudounilaterality, Simple-Rate Variables, and Other Ills to Which Interaction Research Is Heir.” *Journal of Personality and Social Psychology* 46 (6): 1335. <https://doi.org/10.1037/0022-3514.46.6.1335>.
- Dworkin, J. 2018. “Adolescents as the Family Technology Innovators.” In *Families and Technology*, edited by Van Hook, J., McHale, S. M., and King, V., 23–36. Cham: Springer.
- Feng, Y., Y. Sun, N. Wang, and X.-L. Shen. 2025. “Co-owned Information Disclosure and Collective Privacy Calculus on Social Network Platforms: The Moderating Role of Information Ownership.” *Internet Research* 35 (3): 1154–1180. <https://doi.org/10.1108/INTR-03-2023-0205>.
- Feng, Y., Y. Zhang, and L. Li. 2023. “Collective Impression Management and Collective Privacy Concerns in co-owned Information Disclosure: The Mediating Role of Relationship Support and Relationship Risk.” *Library Hi Tech* 43 (2/3): 568–589. <https://doi.org/10.1108/LHT-05-2023-0196>.
- Franz, A., and A. Benlian. 2022. “Exploring Interdependent Privacy – Empirical Insights into Users’ Protection of Others’ Privacy on Online Platforms.” *Electronic Markets* 32 (4): 2293–2309. <https://doi.org/10.1007/s12525-022-00566-8>.
- Ghose, A., H. A. Lee, W. Oh, and Y. Son. 2024. “Leveraging the Digital Tracing Alert in Virus Fight: The Impact of COVID-19 Cell Broadcast on Population Movement.” *Information Systems Research* 35 (2): 570–589. <https://doi.org/10.1287/isre.2022.0117>.
- Hertlein, K. M., and M. L. Twist. 2019. *The Internet Family: Technology in Couple and Family Relationships*. New York, NY: Routledge.
- Hiller, J., F. Bélanger, M. Hsiao, and J.-M. Park. 2008. “POCKET Protection.” *American Business Law Journal* 45 (3): 417–453. <https://doi.org/10.1111/j.1744-1714.2008.00061.x>.
- Hutchins, H. J. 2020. “COVID-19 mitigation behaviors by age group – United States, April – June 2020. MMWR.” *Morbidity and Mortality Weekly Report*, 69.
- Iacovou, C. L., R. L. Thompson, and H. J. Smith. 2009. “Selective Status Reporting in Information Systems Projects: A Dyadic-Level Investigation 1.” *MIS Quarterly* 33 (4): 785–810. <https://doi.org/10.2307/20650327>.
- Johnson, M. K., S. Mollborn, and C. Horne. 2025. “Yes, Parents, It Reflects on You: Norms and Metanorms Regulating Teen Daughters and Parents.” *Journal of Marriage and Family* 87 (4): 1783–1799. <https://doi.org/10.1111/jomf.13090>.
- Kennedy, C., N. Hatley, A. Lau, A. Mercer, S. Keeter, J. Ferno, and D. Asare-Marfo. 2022. “Strategies for Detecting Insincere Respondents in Online Polling.” *Public Opinion Quarterly* 85 (4): 1050–1075. <https://doi.org/10.1093/poq/nfab057>.
- Kenny, D. 2006. “intodyad.”
- Kenny, D. A., D. A. Kashy, and W. L. Cook. 2006. *Dyadic Data Analysis*. New York, NY: Guilford Press.
- Ladyzhets, B. 2021. “We investigated Whether digital contact tracing actually worked in the US.” MIT Technology Review. Retrieved July 17, 2023, from <https://www.technologyreview.com/2021/06/16/1026255/Us-digital-contact-tracing-exposure-notification-analysis/>.
- Laufer, R. S., and M. Wolfe. 1977. “Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory.” *Journal of Social Issues* 33 (3): 22–42. <https://doi.org/10.1111/j.1540-4560.1977.tb01880.x>.
- Lazarsfeld, P., and N. Henry. 1968. “Latent Structure Analysis”.
- Li, Y. 2012. “Theories in Online Information Privacy Research: A Critical Review and an Integrated Framework.” *Decision Support Systems* 54 (1): 471–481. <https://doi.org/10.1016/j.dss.2012.06.010>.
- Mattke, J., L. Müller, C. Maier, and H. Graser. 2018. “Avoidance of Social Media Advertising: A Latent Profile Analysis.” Proceedings of the 2018 ACM SIGMIS Conference on Computers and People Research, Buffalo-Niagara Falls NY USA.
- McCutcheon, A. L. 1987. “Latent Class Analysis.”
- Miller-Goldwater, H. E., and V. R. Simmering. 2022. “Examining the Role of External Language Support and Children’s own Language use in Spatial Development.” *Journal of Experimental Child Psychology* 215:105317. <https://doi.org/10.1016/j.jecp.2021.105317>.
- Nam, J. 2014. “Understanding the Motivation to use web Portals.” *Computers in Human Behavior* 36:263–273. <https://doi.org/10.1016/j.chb.2014.03.074>.
- Oberski, D. 2016. “Mixture Models: Latent Profile and Latent Class Analysis.” In *Modern Statistical Methods for HCI*, edited by J. Robertson and M. Kaptein, 275–287. Cham, Switzerland: Springer.
- Ogolsky, B. G., A. M. Whittaker, and J. K. Monk. 2019. “Power in Families.” In *Power in Close Relationships*, edited by C. R. Agnew and J. J. Harman, 143–172. Cambridge, UK: Cambridge University Press.
- Ozdemir, Z. D., Jeff Smith, H. Benamati, and J. H. 2017. “Antecedents and Outcomes of Information Privacy Concerns in a Peer Context: An Exploratory Study.” *European Journal of Information Systems* 26 (6): 642–660. <https://doi.org/10.1057/s41303-017-0056-z>.
- Patterson, W. 2021. “Analysis of Risks to Data Privacy for Family Units in Many Countries.” In *Advances in Human Factors in Robots, Unmanned Systems and Cybersecurity*, edited by M. Zallio, C. Raymundo Ibañez, and J. H. Hernandez268, 215–222. Cham, Switzerland: Springer International Publishing. https://doi.org/10.1007/978-3-030-79997-7_27.
- Pearson, J. M., C. S. McCahon, and R. T. Hightower. 1995. “Total Quality Management. Are Information Systems Managers Ready?” *Information & Management* 29 (5): 251–263. [https://doi.org/10.1016/0378-7206\(95\)00028-0](https://doi.org/10.1016/0378-7206(95)00028-0).
- Peel, D., and G. J. McLachlan. 2000. “Robust Mixture Modelling Using the t Distribution.” *Statistics and Computing* 10:339. <https://doi.org/10.1023/A:1008981510081>.
- Petronio, S. 2010. “Communication Privacy Management Theory: What Do We Know about Family Privacy Regulation?” *Journal of Family Theory & Review* 2 (3): 175–196. <https://doi.org/10.1111/j.1756-2589.2010.00052.x>.
- Petronio, S. 2013. “Brief Status Report on Communication Privacy Management Theory.” *Journal of Family Communication* 13:6–14. <https://doi.org/10.1080/15267431.2013.743426>.

- Podsakoff, P. M., S. B. MacKenzie, J.-Y. Lee, and N. P. Podsakoff. 2003. "Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies." *Journal of Applied Psychology* 88 (5): 879. <https://doi.org/10.1037/0021-9010.88.5.879>.
- Podsakoff, P. M., N. P. Podsakoff, L. J. Williams, C. Huang, and J. Yang. 2024. "Common Method Bias: It's bad, It's Complex, It's Widespread, and It's Not Easy to fix." *Annual Review of Organizational Psychology and Organizational Behavior* 11 (1): 17–61. <https://doi.org/10.1146/annurev-orgpsych-110721-040030>.
- Roberson, P. N. E., K. A. Lenger, T. Gray, J. Cordova, and K. C. Gordon. 2020. "Dyadic Latent Profile Analyses and Multilevel Modeling to Examine Differential Response to Couple Relationship Education." *Journal of Family Psychology* 34 (7): 879–885. <https://doi.org/10.1037/fam0000667>.
- Romine, V. 2021. "Crime, DNA, and Family: Protecting Genetic Privacy in the World of 23andMe." *Ariz. St. LJ* 53:367–397.
- Rosenberg, J. M., V. C. Lissa, J. A. Schmidt, P. N. Beymer, D. Anderson, and M. J. Schell. 2021. "tidyLPA: Easily Carry Out Latent Profile Analysis (LPA) Using Open-Source or Commercial Software."
- Schwarz, G. 1978. "Estimating the Dimension of a Model." *The Annals of Statistics* 6 (2): 461–464. <https://doi.org/10.1214/aos/1176344136>.
- Servick, K. 2020. "COVID-19 contact tracing apps Are coming to a phone near You. How Will We know Whether They work?" *Science Magazine*. <https://www.sciencemag.org/news/2020/05/countries-around-world-Are-rolling-out-contact-tracing-apps-contain-coronavirus-How>.
- Shkedy, J. 2020. "Do Virtual Classrooms Encroach on Family Privacy Rights?" *Cardozo Arts & Entertainment Law Journal* 244.
- Smith, H. J., T. Dinev, and H. Xu. 2011. "Information Privacy Research." *An Interdisciplinary Review. MIS Quarterly* 35 (4): 989–1015.
- Smith, H. J., S. J. Milberg, and S. J. Burke. 1996. "Information Privacy: Measuring Individuals' Concerns about Organizational Practices1." *MIS Quarterly* 20 (2): 167–196. <https://doi.org/10.2307/249477>.
- Spurk, D., A. Hirschi, M. Wang, D. Valero, and S. Kauffeld. 2020. "Latent Profile Analysis: A Review and "How to" Guide of Its Application within Vocational Behavior Research." *Journal of Vocational Behavior* 120:103445. <https://doi.org/10.1016/j.jvb.2020.103445>.
- Steinberg, L. D. 2014. *Age of Opportunity: Lessons from the new Science of Adolescence*. Boston, MA: Houghton Mifflin Harcourt.
- Tein, J.-Y., S. Coxé, and H. Cham. 2013. "Statistical Power to Detect the Correct Number of Classes in Latent Profile Analysis." *Structural Equation Modeling: A Multidisciplinary Journal* 20 (4): 640–657. <https://doi.org/10.1080/10705511.2013.824781>.
- Trepte, S., M. Scharnow, and T. Dienlin. 2020. "The Privacy Calculus Contextualized: The Influence of Affordances." *Computers in Human Behavior* 104:106115. <https://doi.org/10.1016/j.chb.2019.08.022>.
- Udo, G., and T. Guimaraes. 1994. "Empirically Assessing Factors Related to DSS Benefits." *European Journal of Information Systems* 3 (3): 218–227. <https://doi.org/10.1057/ejis.1994.22>.
- Whitney, L. 2020. "Most Americans say 'No' to Coronavirus Contact Tracing Apps." *Software*. <https://www.techrepublic.com/article/Most-americans-say-No-to-coronavirus-contact-tracing-apps/>.
- Wickham, H., R. François, L. Henry, K. Müller, and Rstudio. 2022. "dplyr: A Grammar of Data Manipulation."
- Wickham, H., and Rstudio. 2022. "tidyverse: Easily Install and Load the 'Tidyverse'."
- Xu, H., H. H. Teo, B. C. Y. Tan, and R. Agarwal. 2010. "The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services." *Journal of Management Information Systems* 26 (3): 135–173.
- Zhang, M., O. Turel, and A. Zöll. 2026. "Group Closeness Effects on co-owned Information Sharing: A Multilevel Perspective." *International Journal of Information Management* 86:102977. <https://doi.org/10.1016/j.ijinfomgt.2025.102977>.
- Zhang, M., and H. Zhu. 2025. "'Their Privacy Matters Too!' a Self-other Calculus Perspective on Disclosure of Others' Information on Social Media: The Influence of Relationship Closeness and Affect." *Computers in Human Behavior* 168:108665. <https://doi.org/10.1016/j.chb.2025.108665>.
- Zöll, A., A. Franz, and O. Turel. 2026. "Dyadic Privacy Management: The Influence of Dyadic Privacy Norms on the Disclosure of Co-owned Information in Romantic Relationships." *Information & Management* 63 (2): 104301. <https://doi.org/10.1016/j.im.2026.104301>.

Appendices

Appendix A: survey measures.

Table A1. Survey Measures and Key Definitions

Construct	Items	Source
CTA privacy concern – self [1-5; not at all-very concerned] <i>Definition:</i> Concerns about misuse of personal information submitted to a CTA	<ol style="list-style-type: none"> 1. I am concerned that the information I submit when using a contact tracing app could be misused. 2. I am concerned that people can find private information about me from using a contact tracing app. 3. I am concerned about submitting information to a contact tracing app because of what others might do with it. 4. I am concerned about submitting information to a contact tracing app because it could be used in a way I did not foresee. 	Adapted from Dinev and Hart (2006)
CTA privacy concern – family [1-5; not at all-very concerned] <i>Definition:</i> Concerns about misuse of family member information submitted to a CTA	<ol style="list-style-type: none"> 1. I am concerned that the information my family members submit when using a contact tracing app could be misused. 2. I am concerned that people can find private information about other members of my family from using a contact tracing app. 3. I am concerned about my family members submitting information to a contact tracing app because of what others might do with it. 4. I am concerned about my family members submitting information to a contact tracing app because it could be used in a way we did not foresee. 	Adapted from Dinev and Hart (2006)
CTA benefits [Summative] <i>Definition:</i> Benefits received from utilising a CTA	<p>Which of the following benefits would convince you to use a contact tracing app during the COVID-19 pandemic? (Mark all that apply)</p> <ol style="list-style-type: none"> 1. More freedom to travel. 2. More comfortable going to school or work. 3. More comfortable completing required errands (store, doctor, etc.). 4. Feeling more secure that I would not get sick. 5. Feeling more secure that my family would not get sick. 6. Socialising outside my home. 7. More accurate data about the spread and number of cases. 8. By using the app, I can make an important contribution to my personal health. 9. By using the app, I can make an important contribution to the health of the population. 10. 10. The pandemic will end sooner. 	Adapted from (Pearson, McCahon, and Hightower 1995)
Intention to use [1-5; not likely at all – very likely] <i>Definition:</i> Intention to use a CTA	<p>If a contact tracing app is available but you are not required to use it, how likely would you be to use it?</p>	Adapted from Nam (2014)
Related health behaviours [1-5; never-always] <i>Definition:</i> Recommended behaviours for COVID-19 mitigation not related to CTA	<p>Please rate how much you are doing each of the following behaviours during the COVID-19 pandemic?</p> <ul style="list-style-type: none"> • I stay six feet from others outside of my home. • I avoid public gatherings. • I stay at home as much as possible. 	Adapted from Udo and Guimaraes (1994) by following guidelines from Hutchins (2020) and World Health Organization ⁵
Marker [1-5 strongly disagree-agreee]	<ol style="list-style-type: none"> 1. I prefer blue to other colors 2. I like the color blue 3. I like blue clothes 	(Miller-Goldwater and Simmering 2022)
Demographics	<p>gender, race/ ethnicity, marital status, education, employment, number of adults and children in household, school grade, income, zip</p>	
Collective Privacy	<p>Definition: Privacy considerations involving groups rather than individuals, where shared norms, relationships, and interdependence shape disclosure decisions.</p>	
Dyadic-Level Data	<p>Definition: data from related groups of two distinguishable individuals (Kenny, Kashy, and Cook 2006).</p>	
Interdependent Privacy	<p>Definition: Decisions in which one person's choices affect others' privacy (Franz and Benlian 2022).</p>	
Latent Profiles Analysis (LPA)	<p>Definition: A statistical technique used to identify hidden subgroups (profiles) based on patterns in continuous variables.</p>	
Privacy Calculus	<p>Definition: A decision-making process in which individuals weigh the perceived risks (privacy concerns) against the perceived benefits when deciding whether to disclose information (Bélanger et al. 2022).</p>	

Pearson, McCahon, and Hightower (1995); Nam (2014); Udo and Guimaraes (1994); Hutchins (2020).

⁵<https://www.who.int/emergencies/diseases/novel-coronavirus-2019/advice-for-public>

Appendix A2: reliability and validity

We tested scale reliability and validity for the measures used in the latent profile analyses for Times 1 and 2 using the covariance-based structural equation modeling module in SmartPLS 4.1.0.1 (See Table A2). Reliability is not reported for CTA benefits as it was a summative scale and for intention to use CTA as this was a single-item scale.

Table A2. Construct Reliability

Construct	Alpha	Time 1		Alpha	Time 2	
		CR	AVE		CR	AVE
Parent – Privacy Concern Family	0.986	0.986	0.948	0.984	0.984	0.939
Parent – Privacy Concern Self	0.970	0.970	0.890	0.970	0.970	0.891
Teen – Privacy Concern Family	0.985	0.985	0.942	0.991	0.991	0.963
Teen – Privacy Concern Self	0.978	0.979	0.919	0.986	0.986	0.946

CR.: Composite Reliability; AVE.: Average Variance Extracted.

Tables A3 and A4 report discriminant validity results using the Heterotrait-Monotrait (HTMT) ratios. Discriminant validity was observed for most of the scales with HTMT ratios well below the 0.9 cutoff. There were two potential discriminant validity issues. Parent privacy concern for the family and parent privacy concern for the self had a HTMT ratio of 0.972 at time 1 and 0.985 at time 2. Similarly, teen privacy concern for the family and teen privacy concern for the self had HTMT ratios of 0.941 at time 1 and 0.977 at time 2. This is not completely unexpected as we anticipated that concern for oneself would be consistent with concern for a person’s family. Additionally, we do not observe discriminant validity issues between the parent and teen versions of the scale.

Table A3. Discriminant Reliability HTMT Ratio – Time 1.

Construct	P – CTAB	P – PCF	P – IUCTA	P – PCS	T – CTAB	T – PCF	T – IUCTA
Parent – CTA Benefits							
Parent – Privacy Concern Family	0.323						
Parent – Intention to Use CTA	0.478	0.352					
Parent – Privacy Concern Self	0.328	0.972	0.360				
Teen – CTA Benefits	0.697	0.227	0.430	0.225			
Teen – Privacy Concern Family	0.184	0.665	0.260	0.610	0.178		
Teen – Intention to Use CTA	0.454	0.315	0.630	0.331	0.577	0.337	
Teen – Privacy Concern Self	0.217	0.653	0.250	0.606	0.195	0.941	0.389

Table A4. Discriminant Reliability HTMT Ratio – Time 1 **Table A5.** Discriminant Reliability HTMT Ratio – Time 2.

Construct	P – CTAB	P – PCF	P – IUCTA	P – PCS	T – CTAB	T – PCF	T – IUCTA
Parent – CTA Benefits							
Parent – Privacy Concern Family	0.323						
Parent – Intention to Use CTA	0.478	0.352					
Parent – Privacy Concern Self	0.328	0.972	0.360				
Teen – CTA Benefits	0.697	0.227	0.430	0.225			
Teen – Privacy Concern Family	0.184	0.665	0.260	0.610	0.178		
Teen – Intention to Use CTA	0.454	0.315	0.630	0.331	0.577	0.337	
Teen – Privacy Concern Self	0.217	0.653	0.250	0.606	0.195	0.941	0.389

Appendix A3: summary of key contributions

Table A5. Summary of key contributions compared to existing knowledge

Area	Existing Knowledge in the Field	Contribution of This Study
Collective / Interdependent Privacy	Privacy calculus and privacy concerns are predominantly conceptualised and measured at the individual level; limited empirical work examines privacy as a shared, relational, or collective process.	Demonstrates parent – teen dyads form shared, collective privacy orientations; extends privacy calculus beyond the individual to account for joint evaluations of risks and benefits.
Stability of Privacy Calculus Over Time	Prior work acknowledges privacy beliefs may change with context but lacks longitudinal evidence of stability at the collective level.	Shows dyadic privacy profiles remain stable across time, indicating enduring collective norms.
Methodological Advancement: Latent Profile Analysis	Variable-centered methods dominate; LPA rarely used in privacy research and rarely applied to dyads.	Introduces LPA to uncover collective privacy patterns not observable through individual-level or aggregated analyses.
Intra-Dyad Differences Within Collective Alignment	Research often assumes family-unit homogeneity or analyzes members separately.	Shows parents and teens may differ in concern levels, yet still form coherent collective orientations.
Behavioural Generalisation Beyond Technology Use	Privacy calculus typically applied only to disclosure or technology adoption.	Demonstrates that dyadic profiles predict broader protective behaviours beyond technology use.
Support for Multilevel Theories of Privacy	Multilevel privacy theories exist conceptually but lack empirical grounding.	Provides empirical support linking individual, dyadic, and collective privacy processes.