Proceedings of the 5th International Conference on Financial Technology and Business Analysis (ICFTBA 2026)
DOI: 10.54254/2754-1169/2026.39327

Perceptions of Apple Native Privacy Tools among International High-School Students: A Qualitative Study

Jinling Tian

New Oriental School, Jinan, China
jinling@outlook.com

Abstract. This exploratory qualitative study examines the perceptions of international high-school students of Apple's native privacy tools and their digital-privacy experiences in relation to campus. Four young adults (16-20 years old) were interviewed using semi-structured interviews and reflexive thematic analysis with privacy calculus, boundary regulation, usable-privacy and AIDA models was used. Results show that there are real-world campus privacy risks that pose threats to adolescents. Participants prefer privacy features that do not require much effort and are presented in the context of scenarios, but find that advanced features are discovered less and are technically complicated. They are still dependent on technical evidence and rumours swirling around the Internet about Apple's protection of their privacy. It also reveals a mismatch between teenagers' privacy demands and the current privacy communication strategies adopted by technology firms. This research provides initial practical marketing implications for technology brands and helps to expand research on privacy among adolescents, although the results are limited by the sample size and the results cannot be generalized widely.

Keywords: high-school students, digital privacy, Apple privacy tools, usable privacy

1. Introduction

In the digital age, international high school students have unique cross-border privacy risks. This age group of teens faces greater challenges with digital privacy than other groups of students when they use mixed social platforms, cross-regional data transportation, and hybrid learning environments. Teenagers (16-20 years old) attending international high schools are constantly exposed to risk for their privacy when using digital technologies in their daily school lives, such as the potential leakage of information over public school Wi-Fi networks, sharing of private photos and homework drafts on social media, and tracking by third-party learning apps [1]. This demographic makes extensive use of TikTok and Instagram for creating content and engaging socially for campuses, but there is no formal guidance for them to use; lengthy privacy documents and technical explanations from brands do not align with the preferences for short, visual media that adolescents have [2]. As a brand centering privacy as its core competitive value, Apple has built a full set of built-in privacy tools, such as App Tracking Transparency, private photo albums and App Privacy Report, which grant users full control over personal digital data [3]. But, most of Apple official marketing is based on textual webpages, and there is no campus-specific scenarios, so the awareness of teen population is

© 2026 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

DOI: 10.54254/2754-1169/2026.39327

low and the positive evaluation of consumer is limited for these privacy features. Researchers have validated the privacy paradox among children: teens are highly concerned about chat history and information leaks from school files, but they do not take steps to protect their information on the devices unless it is easy to do so [4].

There are a number of key research questions that are under-researched. Although short video platforms have been found to be effective to disseminate simplified technical knowledge to Generation Z, there are few studies on designing TikTok campaigns themed with campus to popularize mobile privacy functions for international high school students [5]. While there are various studies examining iOS privacy mechanisms in their technical context, they fail to consider the positive impact of targeted social media content on the brand perception of the teen users whose families consider data security as their main criteria when purchasing devices, yet not the price [6]. Few studies have been conducted on international students' particular campus privacy concerns and there are few communication strategies specifically geared towards this mobile adolescent population.

The present study aims to fill above gaps by interviewing 16–20-year old international high school students and investigating how campus themed short videos can simplify Apple's multi-layered Privacy tools, diminish the risk of campus data leakage, and create positive brand evaluation by teenagers. This research applies the Segmentation-Targeting-Positioning (STP) framework to clarify teen consumer positioning and optimises strategies through the four-Ps (Product-Price-Place-Promotion) marketing mix. It provides practical social media marketing guidelines for tech brands and extends privacy research by verifying that narrative-driven short videos convert abstract iOS privacy features into intuitive, valuable brand benefits for international adolescent users.

Based on the identified research gaps, this study addresses the following research questions: How do participants describe digital privacy risks and privacy-management practices in everyday campus life? How do participants understand and evaluate Apple privacy features in relation to campus privacy needs? What factors strengthen or weaken trust in Apple's privacy commitments? What short-video scenarios, evidence and instructional elements make privacy communication attention-grabbing, understandable, credible and actionable?

2. Literature review

2.1. Definition of adolescent campus digital privacy management

Teenagers aged 16-20 spend most of their school time connected to digital devices, and they face unique privacy risks inside international high school campuses. Digital privacy risk refers to the chance that sensitive personal data stored, transmitted or collected by smartphones suffers unauthorised access, tracking or leakage, including location data, school assignments, private photos and personal chat records [7] .Common risks include data tracking on shared public Wi-Fi, accidental leaks of homework drafts and private photos, and unauthorized data collection from third-party learning apps [8] . Interview-based research on young TikTok users confirms that adolescents clearly know these risks exist, and they take simple actions to protect their personal information online. Typical self-management practices include limiting audience access to posted videos and avoiding sharing sensitive school materials in public posts.

However, existing research has clear context limits. Most interview samples come from European domestic high schools, not Canadian international student groups who frequently switch between cross-border social platforms and shared classroom devices. Many studies only observe teenagers' passive risk avoidance, and they rarely discuss how built-in mobile device tools can support their

DOI: 10.54254/2754-1169/2026.39327

daily privacy management on campus. This gap highlights the core value of the current research, which explores the real campus privacy challenges experienced by Canadian international high school students and how Apple's built-in privacy tools can address such digital security concerns.

2.2. Review on adolescent privacy perception and usable privacy

Usable privacy research is about the usability of technical privacy functions for the end user. With a clear official design objective to place the data under full control of the users, Apple introduced a whole suite of native privacy features, such as App Tracking Transparency, App Privacy Report and hidden private photo albums. Several user studies demonstrate that most young users have positive general impressions of these functions since they prevent hidden tracking of apps as well as locking personal media without additional compensation.

However, there are always some common constraints in the literature. First, many of the usability tests are conducted with adults, and not with groups of teenage high school students [9], thus the results achieved in the tests cannot be fully transferred to international high school users within the age range of 16 – 20 years. Secondly, there is a disconnect between understanding: while young users can easily grasp simple one-click privacy settings to protect their campus information, data reports with a lot of technical jargon are cognitively overwhelming and confuse teenagers.

2.3. Theoretical framework

The privacy paradox and privacy calculus theory are two major theories attempting to depict the dichotomy between teenagers' privacy concerns and actual protective behaviors. The privacy paradox (PP) refers to a commonly observed trend whereby young people are concerned about data leakage [10]. This gap is the essence of this research, which examines the actual challenges of campus privacy faced by international high school students in Canada and the ways that Apple's inbuilt privacy features can be used to address some of the privacy issues Canadian international high school students encounter online. This gap can also be understood in terms of 'cost-benefit' reasoning in the sense of privacy calculus theory, a sociological and psychological model to explain how people can rationally assess the potential benefits against the potential risks of sharing their personal information [11].

In determining whether or not to post campus content, share information, or learn privacy tools, teens consider three main aspects: social benefits, potential costs of photo or file exposure, and time required to become proficient in complex device controls [12]. When teens are concerned about privacy, they will probably opt to ignore privacy protection if the operation's cost is too steep.

Boundary Regulation Theory is a psychological theory that views privacy as a balancing and adjusting activity developed in 1975 by psychologist Irwin Altman. The theory states that during interpersonal interactions, people continuously adjust the boundaries between themselves and others based on their personal needs for openness or concealment, just like switching a valve, so as to reach the most comfortable social state. Communication Privacy Management (CPM), an extended framework also referred to as boundary regulation theory, further supplements an interpersonal perspective for this analysis [13] . This theory views privacy as a flexible boundary that users adjust based on different audiences, such as classmates, teachers and family members. Recent youth-focused interview research finds that teens hope to control who can view their school photos and chat records, yet most standard mobile systems lack easy tools to draw clear sharing boundaries. Apple's private photo albums and tracking restriction features match this demand for boundary

DOI: 10.54254/2754-1169/2026.39327

control, allowing young users to flexibly decide what personal campus data to disclose to peers, teachers and third-party applications.

Based on the literature review, several critical research gaps are identified. Existing adolescent privacy studies primarily focus on local student groups rather than cross-border international high school cohorts, neglecting their unique campus privacy risks [14]. Furthermore, privacy paradox and privacy calculus theories merely explain adolescents' passive protective behaviours, without exploring how user-friendly brand privacy tools reduce protection costs and reshape user attitudes. Relevant usable privacy research also relies heavily on adult participants and textual materials. To address these gaps, this study adopts semi-structured interviews guided by four research questions. Thematic analysis, grounded in privacy calculus, boundary regulation, usable privacy and the Attention-Interest-Desire-Action (AIDA) model, is applied to generate targeted marketing insights for adolescent-oriented privacy promotion.

3. Methodology

3.1. Research design

This paper uses exploratory qualitative research.It collects data through semi-structured one-on-one interviews and applies reflexive thematic analysis to process interview transcripts. Reflexive thematic analysis is a widely-used qualitative approach for identifying, organising and interpreting meaningful patterns within qualitative text data. This paper follows the six-phase analytical procedure defined by Braun and Clarke to conduct coding, theme development and result interpretation. The research mixes deductive and inductive coding. Deductive codes come from core theories including privacy calculus, boundary regulation, and usable privacy, which act as sensitizing concepts to guide analysis. Inductive codes are created directly from participants' original words without pre-set assumptions. Specifically, the research applies hybrid deductive-inductive analysis. Deductive (theory-driven) analysis is where coding and interpretation are guided by pre-existing theories, conceptual frameworks or research questions. By contrast, inductive (data-driven) analysis is an approach that generates codes directly from participants' raw statements, without rigid pre-imposed theoretical categories [15].The study follows the Consolidated Criteria for Reporting Qualitative Research reporting standard to keep the whole research process transparent [16]. Four open-ended research questions guide all data collection and analysis work.

3.2. Participants and sampling

The population in this study was four respondents who were determined by using non-probability sampling technique namely convenience sampling technique where the respondents were accessible and readily available to the researcher. Everyone in the groups is eligible: all are currently in international high schools and use Apple mobile devices, and are between 16 and 20 years of age. The respondents were selected from the students of various social groups within the international campuses. Ahead of the official interviews, researchers validated the use of iPhones and the minimum experience of each participant with Apple privacy features.

3.3. Interview procedure

A uniformed neutral semi-structured interview guide was used for all interviews in this study. One student was used as a pretest for the guide to eliminate leading questions. The same steps were

DOI: 10.54254/2754-1169/2026.39327

followed in each interview. Initially, researchers gave explanation on the purpose of the study and obtained informed written consent from all the participants. The consent to audio recording and complete transcript was obtained from all participants. Secondly, basic background information, such as age, daily use of devices and familiarity with Apple, was gathered. Thirdly, the participants were asked to share real-life digital privacy risks that they encountered in school. Fourth, neutral follow up questions were used to solicit the participants' understanding, feelings and doubts about the video content and Apple's privacy features. The interview time ranged from 15 to 20 minutes. All recordings were fully transcribed and all personal details such as names of schools and individuals were deleted prior to anonymisation. Encrypted folders of all audio and transcripts.

3.4. Data analysis

Relexive thematic analysis was used with six phases to analyse the data. In line with the six-phase reflexive thematic analysis process proposed by Braun and Clarke , the researchers started by familiarizing themselves with the data by repeatedly reading all interview transcripts and taking notes about initial thoughts and ideas in the form of reflexive memos. Then all the text was systematically coded semantically and latently, with deductive codes indicating content that is related to privacy cost, boundary control and usability, and with inductive codes identifying emerging patterns, such as the impact of rumours on the Web on brand trust. Codes were then sorted into related groups to generate candidate themes, which were then cross-checked with all of the transcripts for internal consistency and to find counter-examples. Each final theme was clearly defined and related to the four main research questions and supporting evidence and analytical interpretations were then summarised in formal result paragraphs. To ensure the trustworthiness of the analysis, full coding log and a theme map were kept.

4. Results and discussion

Six common themes emerged from the four transcripts of the interviews. All of the results are restricted to this small sample and therefore cannot be generalized.

The first theme the participants described concrete "digital privacy risks" that were campus related. Potential risks were public Wi-Fi tracking, stolen homework photos, leaked location information and third party learning app data collection. Fully 100% of the four students indicated that concerns about privacy were based on real-life experiences rather than ideas of technology. In the second theme, students chose low effort boundary control tools. Password locks and one-click permission switches and hidden photo albums were readily accepted. Multi-step settings were uncommon, suggesting that privacy calculus applies to these settings. For the third theme, Apple's privacy tools were only useful in certain campus cases. Private Wi-Fi solved shared network risks, hidden albums provided protection for school photos and assignments. Without clear purposes for a function in everyday life, participants were unable to appreciate the value of functions. Usability in the fourth theme is based on the discoverability of features and previous knowledge about Apple. Easy to use visible tools were easy to master, but App Privacy Report and fine-grained tracking controls were hard to find and understand. Longer usage of Apple led to less confusion. In the fifth theme trust was dependent on the promises Apple makes about privacy. Technical restrictions to app tracking and official privacy policies increased trust, while online speculation regarding cross-border data transfer and legacy flows in the system lowered trust. All respondents had a mixed set of positive and negative attitudes. In theme 6, attention-grabbing short videos focused on relatable campus risk scenarios. Participants indicated that clips of actual school data leaks were easier to

DOI: 10.54254/2754-1169/2026.39327

focus on. But only one of the participants submitted a complete feedback on the complete AIDA phases, evidence for video persuasion remains incomplete.

This section interpretively analyzes the themes arrived at in the light of academic theories already available based on the above empirical findings. It compares, contrasts and relates the findings of this study to previous literature, explains any potential theoretical inconsistencies and research gaps, and develops theoretical and practical implications from this research. The interview results are explained in this section in relation to the literature reviewed, such as privacy calculus, boundary regulation, usable privacy and the AIDA communication model. It also includes study contributions, theoretical and practical implications and clear limitations in research. First, the results confirmed the fundamental idea behind privacy calculus theory. Overall, everyone was deeply concerned about data breaches on campus, yet no one wanted to sacrifice time or convenient digital life on campus by engaging in complex privacy operations. They only selected low tech, low cost protection equipment. The finding contributes to the privacy paradox research that has been done before among European students by demonstrating that international high-school students take into consideration both the practical operational effort needed as well as privacy concerns when making decisions to implement protective behaviors.

Second, the results are in line with the boundary regulation theory. Students desired control over photos and school files and sharing out geo-location data to various audiences such as classmates and teachers. It is there that Apple's secret albums, and app permissions, fit the bill to allow colleges to keep campus data private while making it public. In addition to the above, this study contributes to boundary regulation theory by explaining how tangible mobile-device privacy functions serve as a practical intermediate mechanism that influences and enables teens' psychological boundary negotiation in real-world campus settings, instead of just describing boundary-setting only at the psychological level, which was mostly explored by studies of adult users.

Third, results are in line with research that is usable in privacy. Easy one click controls for daily campus protection is all young users will need. Groups of students struggle to interpret complex data reports that contain a lot of technical jargon and are not very useful. There's a difference between easy, readily available tools and hard to find advanced functions, which means that privacy communication needs to focus on simple features that match the scenarios. This finding brings new aspects into the field of usable-privacy theory, specifically the notion of 'feature discoverability' as an important intermediate conditional factor: technically sophisticated tools that offer privacy protection are not necessarily effective in protecting privacy in practice if made difficult to discover or not closely related to the real-life context in which they are used, as is the case for teenagers' privacy-management behaviour.

Fourthly, conditional brand trust also builds upon trust enabled privacy research. Participants didn't have a positive or negative view of Apple's privacy performance in mind. There was built confidence with official design but unconfirmed on-line rumors undermined confidence. The issue discussed here is a theoretical one that arises from privacy-related trust research in the field of trust-enabled privacy: so far, most of the research on trust and privacy relates to the presence or absence of technical characteristics and official institutional information, and few researchers have considered the role of competing social narratives, such as online rumors. This study incorporates an overlooked social element in the theoretical understanding of adolescent privacy trust, by showing how technical safeguards in combination with official statements and unsubstantiated online rumours lead to mixed, simultaneously positive and negative trust evaluations by users.

DOI: 10.54254/2754-1169/2026.39327

5. Conclusion

To gain an understanding of international high school students' (16-20 years old) experience, perception and mixed feelings about Apple's built-in privacy tools, four semi-structured exploratory interviews were carried out. The findings of the thematic analysis reveal that there are serious digital risks for teenagers in a school context and that teenagers' privacy decisions are based on the concept of privacy trade-offs. While they appreciate features Apple provides that make it easier to draw clear social and learning data boundaries, they find discoverability and technical complexity to be barriers to using advanced privacy capabilities. Trust in Apple's privacy protection changes based on product experience, official information and online rumours. The findings offer tentative theoretical insights and practical recommendations for technology brands developing privacy-related content targeted at student audiences. Readers must remember the small sample and incomplete restrict the transferability of all results. More large-scale and complete data collection is needed to test and expand the themes found in this pilot research.This pilot exploratory study finds that Canadian international high-school students balance privacy risks and practical effort to manage their digital boundaries on campus. While they value accessible mobile privacy tools aligned with real-world school scenarios, conditional trust in device-level privacy protections is shaped by both official technical evidence and conflicting online social narratives. Readers must remember that the small sample and incomplete stimulus-material feedback restrict the transferability of all results. Further large-scale and comprehensive data collection is needed to test, refine and expand upon the themes generated within this pilot research.

There are three main limitations: Firstly, the sample size is only four participants, which is a small sample size study, and can only yield preliminary research results. Results are not necessarily applicable to all international high school students. Second, there was incomplete evidence of interview feedback on the TikTok stimulus materials in that not all the participants provided complete feedback. Third, several interview questions slightly tend to elicit positive brand attitude responses, which could result in mild social-desirability bias in the respondents' responses. Future research could be performed to gather more information from the interviews with larger samples of international students.

References

[1] Gogus, A., & Saygın, Y. (2019). Privacy perception and information technology utilization of high school students. *Heliyon, 5*(5), e01614. https://doi.org/10.1016/j.heliyon.2019.e01614

[2] Muguiro, I., Méndez-Suárez, M., & García-Arias, E. (2026). Do teens understand what they're agreeing to on Insta, TikTok, and X? *Human Behavior and Emerging Technologies*. https://doi.org/10.1155/hbe2/6741473

[3] Wu, X., Hu, L., Zeng, E., Habib, H., & Bauer, L. (2025). Transparency or information overload? Evaluating users' comprehension and perceptions of the iOS App Privacy Report. *NDSS Symposium 2025*. https://www.ndss-symposium.org/wp-content/uploads/6A-s0081-Wu.pdf

[4] Ebert, N., Geppert, T., Strycharz, J., Knieps, M., Hönig, M., & Brucker-Kley, E. (2023). Creative beyond TikToks: Investigating adolescents' social privacy management on TikTok. *Proceedings on Privacy Enhancing Technologies*. https://doi.org/10.56553/popets-2023-0049

[5] Baglione, S., & Tucci, L. A. (2025). Accepting invasive privacy policies in downloading TikTok. *American Marketing Journal, 14*(1). https://digitalcommons.kennesaw.edu/amj/vol14/iss1/3

[6] Kim, J., Wolfe, R., Bhagirathi Subramanian, R., Lee, M.-H., Colnago, J., & Hiniker, A. (2025). Trust-enabled privacy: Social media designs to support adolescent user boundary regulation. *Proceedings of the Twenty-First Symposium on Usable Privacy and Security (SOUPS 2025)*. https://www.usenix.org/conference/soups2025/presentation/kim

[7] Al-Saggaf, Y., & Maclean, J. (2024). Protecting children from smartphone's leakage of security sensitive information. *Teacher Magazine*. https://www.teachermagazine.com/au_en/articles/research-news-students-

DOI: 10.54254/2754-1169/2026.39327

smartphones-and-the-privacy-paradox
[8] Apple. (2025). App privacy features in Apple products. *Apple Official Support*. https://support.apple.com/guide/personal-safety/app-privacy-features-in-apple-products-ipsd4dac4a2c/web
[9] Lin, Y., Juneja, J., Birrell, E., & Cranor, L. F. (2024). Data safety vs. app privacy: Comparing the usability of Android and iOS privacy labels. *Proceedings on Privacy Enhancing Technologies*. https://petsymposium.org/popets/2024/popets-2024-0047.php
[10] Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs, 41*(1), 100-126. https://doi.org/10.1111/j.1745-6606.2006.00070.x
[11] Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*(1), 61-80. https://doi.org/10.1287/isre.1060.0080
[12] Akter, M., Park, J. K., Headrick, C. R., Page, X., & Wisniewski, P. (2024). Calculating connection vs. risk: Understanding how youth negotiate digital privacy and security with peers online. *ACM Transactions on Social Computing*. https://doi.org/10.1145/3757564
[13] Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. State University of New York Press.
[14] Dogruel, L., & Joeckel, S. (2024). Privacy management of pupils in online learning. *Journal of Media & Culture Studies*. https://doi.org/10.1177/20563051241301841
[15] Braun, V., & Clarke, V. (2024). A critical review of the reporting of reflexive thematic analysis. *Health Promotion International*. https://doi.org/10.1093/heapro/daad142
[16] Tong, A., Sainsbury, P., & Craig, J. (2007). Consolidated criteria for reporting qualitative research (COREQ): A 32-item checklist for interviews and focus groups. *International Journal for Quality in Health Care*. https://doi.org/10.1093/intqhc/mzm042