



Information Research – Vol. 31 No. iConf (2026)

From privacy concerns to digital literacies: negotiating trust and authenticity in AI-mediated student records systems

Yang Lu, Yunjie Tang, and Yijia Song

DOI: <https://doi.org/10.47989/ir31iConf64208>

Abstract

Introduction. This study examines how students negotiate privacy concerns in AI-mediated student record systems, focusing on Xuexin.com, China's national digital archive of university student records. Using the antecedent–privacy concern–outcome (APCO) model, privacy practices are framed as forms of information literacy tied to authenticity, trust, and digital inclusion.

Method. Semi-structured interviews were conducted with fifteen students and recent graduates (aged 20–27) between May and July 2025. Interviews lasted 30–60 minutes, face-to-face or online, guided by APCO categories while allowing emergent themes.

Analysis. Directed content analysis with NVivo was applied. APCO codes were refined to include themes of algorithmic opacity, fragile trust, and resistance. Reliability was checked by re-coding 20% of transcripts.

Results. Four antecedents (breaches, literacy, risk, and trust) shaped behaviours from reluctant compliance to withdrawal. Privacy literacy emerged as unevenly distributed, with implications for authenticity and digital inclusion.

Conclusion. Privacy in digital student records systems is best understood as a fragile, uneven literacy practice. Its unequal distribution risks deepening exclusion, raising questions about authenticity, trust, and the conditions for a digitally enlightened society.

Introduction

The digital transformation of student records management has profoundly reshaped how sensitive personal and academic information is stored, accessed, and verified. In China, the Higher Education Student Information Network (CHSI or Xuexin.com) represents the archetype of this shift, transitioning from paper-based records to a hybrid electronic system that enables functions such as online verification reports and automated credential services. In this article, the term student record system refers to centralised, government-managed digital platforms such as CHSI that store, verify, and disseminate official enrolment and degree records for higher education. Functionally, these platforms operate as national online archives of student records rather than as traditional institutional archives preserving a broad range of historical materials.

The integration of artificial intelligence (AI) into such platforms, exemplified by tools like the Xuexin Robot, has further enhanced efficiency by providing around-the-clock verification and responsive user support. Yet these very advances expose student records systems to new vulnerabilities, where automated data processing, opaque algorithms, and large-scale data reuse amplify longstanding privacy concerns.

While previous scholarship has examined digital archives in terms of efficiency, ethics, and trust (Jaillant & Caputo, 2022; Oliver et al., 2011), much less attention has been paid to how AI-mediated systems reshape the conditions of privacy and authenticity in educational contexts. Importantly, students' responses to AI-driven data practices are not only matters of individual preference but also reflections of their information literacies—the knowledge, skills, and critical dispositions required to engage responsibly with digital infrastructures. Privacy literacy, as a key dimension of information literacy (Bawden & Robinson, 2020), becomes central here: students must not only protect personal data but also interpret algorithmic operations, assess the authenticity of system outputs, and decide whether and how to disclose information in environments where disclosure is often mandatory.

Negotiating privacy in AI-mediated student records systems involves more than individual hesitation: it is shaped by breaches of trust, uneven literacies, risk calculations, and fragile reliance on platforms. Positioned within the APCO framework, these dynamics reveal privacy practices as information literacies that continuously remake authenticity, trust, and inclusion, thereby enriching ongoing debates on how digital literacy and ethical awareness are redefined under AI governance.

Theoretical background

The APCO model and its legacy

The antecedent–privacy concern–outcome (APCO) model, first articulated by Smith et al. (1996), has long been employed to explain how individuals perceive privacy risks and translate those perceptions into behaviour. It posits that prior experiences, cognitive judgments, and broader sociocultural contexts give rise to privacy concerns, which then inform disclosure decisions, avoidance, or protective strategies (Benamati et al., 2017; Smith et al., 2011). In environments mediated by AI, the model has been adapted to account for the distinctive tensions between efficiency and vulnerability that algorithmic systems produce (Menard & Bott, 2025). To date, APCO has been applied primarily in commercial and consumer-facing settings, such as e-commerce, social media, and mobile applications, to explain how users translate privacy concerns into disclosure decisions (Sun et al., 2024; Vimalkumar et al., 2021). Much less work has examined public-sector infrastructures and government-managed student record systems.

AI-mediated records platforms as sites of risk and authority

AI alters not only the mechanics of record-keeping but also their epistemic authority. Automated verification, predictive modelling, and large-scale data integration extend the reach of academic

platforms, yet they also deepen opacity and diminish accountability (Croskey et al., 2025). Students seldom know how their records are processed or why certain outputs are privileged as authoritative. Once automated decisions are inscribed into official verification reports, they acquire a truth status that is difficult to challenge, even when errors occur. Moreover, the possibility of data being reused beyond its original purpose destabilises the authenticity of the archive itself. As Jaillant and Caputo (2022) remind us, AI-driven archival systems do not merely enhance efficiency; they reconfigure the very conditions under which truth and trust are constructed.

Privacy literacy as a form of information literacy

Against this backdrop, privacy literacy must be re-imagined as a critical strand of information literacy. Traditionally associated with the ability to recognise risks, evaluate data practices, and apply protective strategies (Sun et al., 2024), privacy literacy in the age of AI requires more than technical precaution. It demands interpretive skill to read algorithmic processes, critical awareness to question automated outputs, and ethical judgment to assess whether digital records are faithful and just (Mooradian et al., 2025). Students' responses to privacy concerns, therefore, are not simply defensive manoeuvres; they are literacy practices that reveal how individuals confront the asymmetrical power embedded in algorithmic infrastructures. To situate privacy within the discourse of information literacy is to acknowledge that the stakes extend beyond individual risk management (Cao et al., 2025). At issue is the possibility of cultivating authenticity, equity, and autonomy in digital education, where AI increasingly governs the boundaries of recognition and participation.

Research method

Research design

This study adopts a qualitative design to resist reducing privacy concerns to quantifiable variables. Privacy is lived, negotiated, and contested, and such dynamics cannot be captured by numerical abstraction alone (Seeman & Susser, 2024). Semi-structured interviews were conducted between May and July 2025 with fifteen participants aged 20–27, all experienced in using AI-mediated student record systems such as Xuexin.com. The sample reflects those most directly bound to these infrastructures: students and recent graduates whose academic futures depend on digital verification. Interviews, lasting 30–60 minutes face-to-face or via Tencent Meeting, followed an APCO-informed guide but also allowed room for themes beyond its categories, such as algorithmic opacity and institutional authority. Informed consent was obtained, and all identifying details were removed.

Analysis followed the principles of directed content analysis (Hsieh & Shannon, 2005), with NVivo used to organise data while interpretation remained open. An initial APCO-based coding scheme was progressively refined as new themes emerged, including doubts about algorithmic truth, frustration with opacity, and resistance strategies such as data minimisation or refusal. To check reliability, 20% of transcripts were re-coded, though the deeper aim was to remain attentive to the ambivalence and critique voiced by participants.

Findings

Privacy breaches: remembered and anticipated

Students' memories of privacy breaches provided the most visceral entry point into their anxieties about AI-mediated record systems. Many described a daily digital environment where boundaries were already fragile, citing unsolicited advertisements, spam calls, and the uncanny precision of commercial algorithms. One participant reflected, *'After I filled in my number on a small app, I kept receiving spam calls. It felt like my personal data was sold immediately'* (P04). Another recalled the discomfort of algorithmic targeting, *'Sometimes after chatting with a friend, I open Douyin and see*

it pushing related content. It's as if the system already knew what I said' (P10). Such experiences cultivated not only distrust but also a form of anticipatory anxiety: if entertainment platforms already breach privacy so effortlessly, the risks posed by AI-mediated verification platforms seemed all the more profound.

Privacy literacy: between awareness and helplessness

The degree to which students could resist or adapt to these risks depended heavily on their privacy literacy. Those with prior training or professional exposure demonstrated sharper awareness, yet they too admitted the limits of agency when confronted with compulsory disclosure. As one student explained, *'I've learned some privacy protection skills during my courses, but it's impossible to fully protect myself. Xuexin requires so much mandatory information that I have no real choice'* (P02). Others revealed uncertainty or resignation, with one participant noting, *'I only know the basics. Most of the time I don't even know what information is being collected, let alone how to stop it'* (P03). Literacy here is revealed as both resource and reminder: a resource for those able to recognise risks, and a reminder of helplessness in the face of infrastructures that permit little refusal.

Risk assessment: calculating exposure in an opaque system

Risk assessment, as narrated by students, resembled less a rational calculation than a precarious balancing act between necessity and opacity. Some practiced forms of partial disclosure, deliberately withholding information when possible. One participant remarked, *'If I don't have to give my full address, I'll leave out part of it. At least that way I share less'* (P01). Yet others described reluctant compliance: *'Even if I sense risks, I still have to provide everything. Without Xuexin, I can't get the verification I need'* (P06). These statements illustrate the paradox of dependence. Students recognise the dangers yet remain compelled to comply, precisely because the archive is indispensable for educational recognition. In AI-mediated contexts, this paradox deepens: the opacity of automated processes renders risks incalculable, so assessment becomes a practice of endurance rather than control.

Platform trust: between authority and scepticism

Trust in the platform emerged as both anchor and fault line. For some, the official status of Xuexin conferred legitimacy: *'I trust Xuexin because it's run by the state. At least it follows the law'* (P11). For others, institutional authority did not erase doubt: *'Even big platforms leak data. Why should I assume Xuexin is any different?'* (P06). Trust, therefore, oscillated between faith in governance and scepticism drawn from broader experiences of digital vulnerability. In AI-mediated record systems, this ambivalence deepens. Automated verification reports acquire the aura of authority, yet the processes that generate them remain inaccessible. Students may submit to such systems out of necessity, but trust itself is fragile, stretched between compliance and suspicion.

Trust in AI-mediated platforms: between authority and scepticism

Trust in AI-mediated platforms emerged as both anchor and fault line. For some, the official status of Xuexin conferred legitimacy: *'I trust Xuexin because it's run by the state. At least it follows the law'* (P11). For others, institutional authority did not erase doubt: *'Even big platforms leak data. Why should I assume Xuexin is any different?'* (P06). Trust therefore oscillated between faith in governance and scepticism drawn from broader experiences of digital vulnerability. In AI-mediated student record systems, this ambivalence deepens further. Automated verification reports acquire the aura of authority, yet the processes that generate them remain opaque. Students may submit to such systems out of necessity, but the trust they place in them is provisional and fragile, easily undermined by the very automation that promises efficiency. To synthesise these themes, Table 1 summarises the antecedent factors shaping students' privacy concerns, their subcategories, the behavioural impacts observed, and illustrative quotes.

Antecedent Factors	Subcategories	Behavioural Impacts	Illustrative Quotes
Privacy Breaches	Everyday intrusions	Cultivates anticipatory anxiety; reduces willingness to disclose	'After I filled in my number on an app, I kept receiving spam calls, as if my data was sold immediately.' (P04)
	Algorithmic surveillance	Heightens sense of being monitored; generates distrust	'Sometimes after chatting with a friend, I open Douyin and it pushes related content, as if it already knew.' (P10)
Privacy Literacy	Knowing (trained awareness)	Enables cautious strategies but limited by compulsory disclosure	'I've learned privacy protection skills, but with Xuexin's requirements it is impossible to fully protect myself.' (P02)
	Not knowing (limited awareness)	Produces resignation and dependence on platform design	'I only know the basics, and most of the time I don't even know what information is collected.' (P03)
Risk Assessment	Perceived risks	Encourages selective disclosure and hesitation	'I try not to fill in personal information unless it is absolutely necessary.' (P05)
	Strategies of reduction	Prompts partial resistance through minimising exposure	'If I don't need to, I leave out part of my home address to share less.' (P01)
Platform Trust	Authority and legitimacy	Increases willingness to comply and disclose	'I trust Xuexin because it's official and governed by laws.' (P11)
	Security scepticism	Fuels reluctance, resistance, or withdrawal from disclosure	'Even major platforms leak data, so I cannot fully trust Xuexin.' (P06)

Table 1. Antecedent factors shaping privacy concerns in AI-mediated student records systems.

From concerns to behaviours: the fragile balancing act

Taken together, these findings suggest that students' privacy concerns are not abstract attitudes but lived negotiations in which disclosure and protection are constantly recalibrated. Privacy breaches instil anxiety, literacy conditions awareness, risk assessment shapes strategies, and trust mediates compliance or resistance. The outcomes manifest along a spectrum: some students engage in reluctant compliance, disclosing out of necessity; others practice cautious engagement, verifying legitimacy before disclosure; still others enact selective resistance, minimising data whenever possible; and a few choose withdrawal from participation, refusing to disclose when risks appear insurmountable. AI mediation amplifies these dynamics by introducing algorithmic opacity and automated authority, transforming privacy from a matter of individual calculation into a structural condition of asymmetrical power. In this fragile balancing act, privacy concerns become the hinge through which literacy, risk, trust, and behaviour converge, shaping how students inhabit and contest AI-mediated student records systems. Figure 1 presents this conceptual model, illustrating how antecedent factors interact to shape privacy concerns, which then lead to divergent behavioural outcomes.

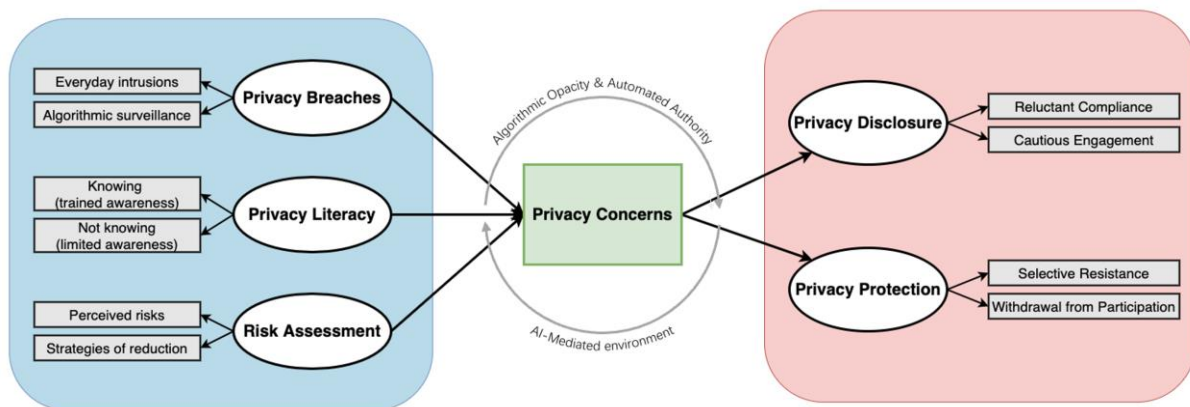


Figure 1. Conceptual model of privacy concerns and behaviours in AI-mediated student records systems.

Discussion

Privacy literacy and digital inclusion

This study positions privacy literacy as a critical dimension of information literacy rather than a narrow set of protective tactics. In AI-mediated student record systems, literacy involves the ability to interpret algorithmic processes, question automated outputs, and make ethical judgments in environments where disclosure often feels mandatory. Students' practices are therefore not only defensive strategies but also cultural and political negotiations within systems of algorithmic governance.

Yet this literacy is unevenly distributed, revealing fractures in digital inclusion. Students with stronger awareness engage in cautious or resistant strategies, while those with limited knowledge often default to reluctant compliance. Such disparities suggest a paradox: infrastructures intended to democratise recognition may, in practice, reinforce inequality (Folk, 2019). The promise of a digitally enlightened society is undermined when the very tools designed to expand access instead deepen exclusion.

From concerns to behaviours

The translation from internal anxiety to external action is the central drama of this study. We see how privacy concerns act as a hinge, swinging individuals toward a spectrum of behaviours. This is not a random process, but a repertoire of responses shaped by the interplay of past traumas, present knowledge, and future stakes. From the resigned submission of reluctant compliance to the subtle defiance of data minimisation, each action is a calculated negotiation on the tightrope of dependence and distrust. By illuminating this journey from concern to practice, this study insists that privacy is not a static attitudinal variable to be measured, but an embodied literacy.

Authenticity, trust, and the future of digital records

At the heart of this dynamic lies a profound paradox of trust and authenticity. The automated verification report, bearing the full weight of institutional authority, is simultaneously a symbol of legitimacy and a source of suspicion. The official seal of the state, once a guarantor of truth, now coexists with the opaque logic of the algorithm, creating a fragile pact of trust that is perpetually at risk of rupture. In this environment, the very architecture of reliability can mask its own fragility, and trust becomes not a stable foundation, but a contested terrain of faith and scepticism.

Navigating this terrain requires us to imagine a future beyond the narrow yardstick of efficiency. A truly enlightened archive is not one that simply processes data faster, but one that cultivates the conditions for critical engagement. This calls for a radical rethinking of institutional responsibility, demanding transparent and contestable algorithmic processes. It requires pedagogical initiatives

that arm students with the critical literacies they need to challenge, rather than merely accept, automated decisions (Han, 2025). Ultimately, the goal is to build governance frameworks that recognise trust as something that must be continuously earned, not simply assumed. Only then can AI-mediated record systems evolve from elegant instruments of compelled compliance into vital infrastructures that support authenticity, equity, and meaningful participation with autonomy and dignity.

Conclusion

Privacy in AI-mediated student record systems emerges not as a settled guarantee but as a fragile negotiation shaped by opacity, compulsion, and asymmetrical authority. Students' practices of disclosure and protection reveal how efficiency often disguises coercion and how authenticity, once anchored in institutional seals, is now a precarious construct sustained by fragile trust in automated processes. To imagine a digitally enlightened archive is therefore to embed privacy literacy as critical agency, to render algorithmic authority transparent and contestable, and to reframe inclusion as participation with autonomy and dignity.

At the same time, this study represents an initial conceptual exploration, grounded in a small set of interviews. Its strength lies in uncovering early patterns of concern and literacy, yet its scope is necessarily limited. Future work will extend this line of inquiry through more in-depth interviews and a large-scale survey, situating AI privacy literacy within the broader cultural environment of China. By tracing how privacy concerns, trust, and literacy practices unfold in specific socio-cultural contexts, subsequent research will deepen our understanding of how digitally mediated record systems can either reproduce exclusion or cultivate conditions of authenticity, equity, and justice.

About the authors

Yang Lu is a Professor and Doctoral supervisor in the School of Cultural Heritage and Information Management at Shanghai University, specialises in archival science, focusing on archival systems, identity, discourse, and information ethics. She has served as a visiting scholar at the University of Tsukuba in Japan and authored two academic monographs and two additional books. She has led multiple research projects funded by the National Social Science Foundation of China and the Ministry of Education. She can be reached at luyang@shu.edu.cn

Yunjie Tang is a PhD candidate in the Department of Information Management at Peking University. An educational foundation has been established with a master's degree in Information Science and a bachelor's degree in Archival Science from Shanghai University. Current research is focused on data culture, governance, and privacy protection within a data-driven society. Publications have been featured in journals, including ILE, LISR, JALIA and information research. Correspondence concerning this article should be addressed to yunjietang@stu.pku.edu.cn

Yijia Song is an assistant librarian at the Library of Fujian Agriculture and Forestry University. Her research interests include privacy concerns and information ethics. She holds an MLIS from Shanghai University. She can be contacted at 000Q825083@fafu.edu.cn

References

- Bawden, D., & Robinson, L. (2020). 'The dearest of our possessions': applying Floridi's information privacy concept in models of information behavior and information literacy. *Journal of the Association for Information Science and Technology*, 71(9), 1030–1043.
<https://doi.org/10.1002/asi.24367>

- Benamati, J. H., Ozdemir, Z. D., & Smith, H. J. (2017). An empirical test of an antecedents–privacy concerns–outcomes model. *Journal of Information Science*, 43(5), 583–600. <https://doi.org/10.1177/0165551516653590>
- Cao, H. J., Lee, H. R., & Peng, W. (2025, April 26–May 1). Empowering adults with AI literacy: using short videos to transform understanding and harness fear for critical thinking. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems (CHI '25)* (pp. 1–8). ACM. <https://doi.org/10.1145/3706598.3713254>
- Croskey, P., Offert, F., Jacobs, J., & Thaler, K. M. (2025, June 23–26). Liberatory collections and ethical AI: reimagining AI development from Black community archives and datasets. In *Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency (FAccT '25)* (pp. 900–913). ACM. <https://doi.org/10.1145/3715275.3732058>
- Folk, A. L. (2019). Reframing information literacy as academic cultural capital: a critical and equity-based foundation for practice, assessment, and scholarship. *College & Research Libraries*, 80(5), 658–672. <https://doi.org/10.5860/crl.80.5.658>
- Han, Y. (2025). People first, preservation later: critical community engagement to activate dialogue-based archives. *Journal of Documentation*, 81(3), 767–787. <https://doi.org/10.1108/JD-09-2024-0210>
- Hsieh, H.-F., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. *Qualitative Health Research*, 15(9), 1277–1288. <https://doi.org/10.1177/1049732305276687>
- Jaillant, L., & Caputo, A. (2022). Unlocking digital archives: cross-disciplinary perspectives on AI and born-digital data. *AI & Society*, 37(3), 823–835. <https://doi.org/10.1007/s00146-021-01367-x>
- Menard, P., & Bott, G. J. (2025). Artificial intelligence misuse and concern for information privacy: new construct validation and future directions. *Information Systems Journal*, 35(1), 322–367. <https://doi.org/10.1111/isj.12544>
- Mooradian, N., Franks, P. C., & Srivastav, A. (2025). The impact of artificial intelligence on data privacy: a risk management perspective. *Records Management Journal*, 35(2), 147–159. <https://doi.org/10.1108/RMJ-06-2024-0013>
- Oliver, G., Chawner, B., & Liu, H. P. (2011). Implementing digital archives: issues of trust. *Archival Science*, 11(3–4), 311–327. <https://doi.org/10.1007/s10502-011-9167-9>
- Seeman, J., & Susser, D. (2024). Between privacy and utility: on differential privacy in theory and practice. *ACM Journal on Responsible Computing*, 1(1), Article 3. <https://doi.org/10.1145/3626494>
- Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, 35(4), 989–1015. <https://doi.org/10.2307/41409970>
- Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: measuring individuals' concerns about organisational practices. *MIS Quarterly*, 20(2), 167–196. <https://doi.org/10.2307/249477>
- Sun, Z., Pan, G., Yang, R., Zang, G., & Zhou, J. (2024). Consumer privacy decision-making in the digital era: an integrative review and taxonomy. *Aslib Journal of Information Management*, Advance online publication. <https://doi.org/10.1108/AJIM-12-2023-0526>

Vimalkumar, M., Sharma, S. K., Singh, J. B., & Dwivedi, Y. K. (2021). 'Okay google, what about my privacy?': User's privacy perceptions and acceptance of voice based digital assistants. *Computers in Human Behavior*, 120, 106763. <https://doi.org/10.1016/j.chb.2021.106763>

© [CC-BY-NC 4.0](#) The Author(s). For more information, see our [Open Access Policy](#).