The Paradox of Intelligent Monitoring Systems of Vocational Education, An Ethical Audit of Stedent Behavior Data Collection at Meishan Vocational College

Danni Zhou [1], Wichai Siriteerawasu[2]
[1]Rattanakosin International College of Creative Entrepreneurship,
Rajamangala University of Technology Rattanakosin
[1]E-mail address: 1672110671107@rmutr.ac.th
[2]Rattanakosin International College of Creative Entrepreneurship,
Rajamangala University of Technology Rattanakosin
[2]E-mail address: wichai.sir@rmutr.ac.th

ABSTRACT

This study conducts an ethical audit of intelligent monitoring systems deployed at Meishan Vocational and Technical College, addressing the core tension between data - driven governance efficiency and student data sovereignty in China's vocational education reform. The research objectives were: (1) to empirically map the current application status of these systems—specifically their deployment scope, multidimensional data types (classroom attention scores, fine-grained technical operation parameters, dormitory routine trajectories), and critically, their highly opaque data circulation pathways; (2) to diagnose the pervasive privacy paradox among students—not as cognitive irrationality, but as a structurally induced "rational compromise" rooted in developmental dependencies (skill certification, internship placement, academic evaluation); and (3) to co-construct a context-sensitive educational data ethics audit framework centered on transparency as the foundational governance lever.

Employing a sequential explanatory mixed-methods design, the study collected quantitative data from 325 valid student questionnaires (stratified random sampling) and qualitative data from 15 in-depth interviews with extreme-case students, supplemented by system log analysis and expert Delphi validation.

Major findings reveal: (1) the system enables comprehensive, multi-scenario data collection yet suffers from severe information asymmetry—only 32% of students knew their training data might be shared externally, and merely 15% understood its purpose; (2) 85% of students expressed high privacy concern, yet 78% accepted data collection, a paradox mediated by perceived usefulness (strongest predictor, $\beta = 0.48$), institutional trust, and crucially, perceived transparency ($\beta = 0.19$, acting as the bridging variable); and (3) the proposed ethical audit framework operationalizes transparency across four pillars—ethical compliance of

collection, security of storage, justifiability of use, and transparency of transfer—and is translated into actionable institutional mechanisms: a statutory Pedagogical Necessity Review Board, a legally enforceable Data Provenance Dashboard for students, and a binding School-Enterprise Data Sharing Charter. This research advances both theory—extending privacy calculus to "development-oriented exchange"—and practice—providing a replicable, value-oriented governance model that reconciles technological capability with pedagogical appropriateness and student rights.

Keywords: Intelligent Monitoring Systems, Privacy Paradox, Educational Data Ethics, Vocational Education, Ethical Audit Framework, Transparency-by-Design

1. Introduction

Intelligent monitoring systems (IMS) are now institutionalized infrastructure in China's vocational colleges—deploying multimodal sensing (video analytics, IoT instrumentation, behavioral profiling) across classrooms, workshops, and dormitories to optimize skill assessment, pedagogical responsiveness, and operational safety. Yet their technical sophistication coexists with profound ethical opacity: at Meishan Vocational and Technical College—a regional exemplar—68% of students remain unaware of data-sharing with enterprise partners; only 15% can articulate its purpose. This is not incidental obscurity, but a systemic compliance gap: the Personal Information Protection Law (PIPL) mandates informed consent and purpose limitation, yet structural dependencies—academic evaluation, internship placement, skill certification—render consent functionally coercive.

The result is a context-specific privacy paradox: 85% of students express high concern about behavioral surveillance ($M = 4.2/5$), yet 78% accept it. Crucially, this disjunction is not cognitive irrationality—it is a development-oriented privacy concession, wherein data compliance is rationally traded for developmental legitimacy. As regression analysis confirms, perceived usefulness ($\beta = 0.48$, $p < 0.001$) outweighs perceived risk ($\beta = -0.22$), while perceived transparency ($\beta = 0.19$) emerges as the critical bridging variable linking institutional trust and risk perception. This reframes the core ethical challenge: not whether IMS can collect data, but whether they can be governed transparently enough to sustain student agency within compulsory educational settings.

Existing frameworks fail this test. Privacy-by-design principles remain abstract; audit tools transplanted from consumer tech ignore vocational education's school-enterprise interdependence and credential-driven power asymmetries. This study therefore advances a context-sensitive ethical audit framework—grounded in empirical deconstruction of the paradox, centered on transparency-as-infrastructure, and operationalized across four governance levers: ethical compliance of collection, security of storage, justifiability of use,

and transparency of transfer. Its contribution is threefold: theoretically, it extends privacy calculus from "convenience trade-off" to "developmental concession"; methodologically, it triangulates quantitative patterns ($R^2 = 0.62$) with deep qualitative mechanisms; and practically, it delivers institutionally embeddable mechanisms—including a statutory Pedagogical Necessity Review Board and a legally enforceable Data Provenance Dashboard—to transform IMS from instruments of disciplinary visibility into scaffolds for co-governed development.

2. Literature Review

2.1 Related Theoretical Foundations

This study is anchored in two interlocking theoretical paradigms that jointly explain the core phenomenon under investigation—the privacy paradox in vocational education's intelligent monitoring ecosystems.

2.1.1 Technical and Managerial Theories of Intelligent Monitoring Systems

Contemporary scholarship frames intelligent monitoring systems not as isolated surveillance tools but as integrated socio-technical infrastructures embedded within institutional governance logics. Domestically, Huang and Chen (2023) conceptualize them as data-driven teaching quality assurance frameworks, where multi-source behavioral data (classroom interaction, practical training metrics, dormitory routines) are aggregated to optimize pedagogical responsiveness and operational safety. Shen (2023) extends this by emphasizing their role as core pillars of internal quality assurance systems in private vocational colleges, particularly where practice-oriented curricula demand real-time skill diagnostics. Technologically, these systems leverage IoT sensor networks (e.g., Yang et al., 2023, on welding torch parameter capture) and computer vision algorithms (Zhao et al., 2023; Deng & Liang, 2024) to generate fine-grained "skill-behavior profiles." Internationally, research underscores contextual adaptation: Karuturi et al. (2025) prioritize safety-critical gas detection in classrooms, while Najmusher et al. (2024) reframe monitoring toward student well-being support rather than managerial control—highlighting a critical divergence between control-oriented and support-oriented design philosophies.

2.1.2 Formation Mechanisms and Explanatory Theories of the Privacy Paradox

The privacy paradox—the disjunction between high privacy concern and high behavioral acceptance—is theorized here through Privacy Calculus Theory (Ou et al., 2023) and Technology Acceptance Model (TAM) (Tan et al., 2023), integrated with contextual privacy theory (Nissenbaum, 2010). Classical privacy calculus posits a rational trade-off between perceived risks and perceived benefits . However, this study advances a vocational-specific recalibration: students' data disclosure is not exchanged for convenience, but for developmental legitimacy—i.e., skill certification, internship placement, and academic evaluation (Gonçalves & Figueiredo, 2025; Hannig et al., 2025). This transforms the paradox

from an individual cognitive failure into a structurally induced rational compromise, moderated by institutional power asymmetry and evaluation dependency (Tan et al., 2023; Ye & Ye, 2023). Crucially, Khattar (2023) provides the ethical counterpoint: privacy-by-design principles—not post-hoc compliance—must mitigate the paradox at its source.

2.2 Critical Review of Empirical Literature

2.2.1 Divergent Research Trajectories: Monitoring Systems vs. Privacy Protection

Existing research exhibits a fundamental epistemological schism. Privacy protection studies (e.g., Wang et al., 2024 on smart homes) focus on end-to-end encryption and local processing within private domains, while intelligent monitoring research (e.g., Wang et al., 2025 on control systems) prioritizes front-end sensing and back-end analytics in semi-public institutional spaces. Legally, privacy scholarship (Mei & Tan, 2024) centers on judicial constraints balancing state power and individual rights, whereas monitoring systems are governed by institutional compliance frameworks emphasizing data minimization and informed consent—yet often lacking enforcement mechanisms. This divergence necessitates a scenario-sensitive ethical framework, not a transplanted consumer-tech model.

2.2.2 Contextual Deficiency: The Meishan Vocational College Gap

While Meishan Vocational and Technical College has deployed multi-scenario monitoring (teaching buildings, workshops, dormitories) with cross-institutional data sharing (e.g., with enterprise partners for talent screening), current research remains narrowly instrumental. Studies focus exclusively on teaching management efficiency—optimizing skill assessment via training data or adjusting pedagogy using classroom behavior analytics (Shen, 2023; Yang et al., 2023). Critically absent is: (a) analysis of the cognitive-behavioral disjunction between students' privacy concerns and data acceptance; (b) an educational data ethics audit mechanism aligned with China's Personal Information Protection Law (PIPL) and Data Security Law; and (c) empirical validation of how vocational-specific pressures (e.g., school-enterprise collaboration, competency-based assessment) reshape privacy trade-offs.

2.3 Conceptual Framework

2.3.1 Theoretical Integration Foundation

The framework fuses Privacy Calculus Theory (risk-benefit perception) and TAM (usefulness-ease of use judgment) to model the vocational education paradox: the tension between rigid skill-development demands and emerging student data subjecthood. This synthesis generates a "context–cognition–behavior–governance" chain, providing the theoretical anchor for deconstructing the privacy paradox and designing the subsequent ethics audit.

2.3.2 Variable Relationships and Logical Chain

The framework specifies causal pathways centered on willingness to accept behavioral data collection as the dependent variable:

Independent Variables: Perceived Usefulness , Perceived Privacy Risk , Institutional Trust , Transparency Perception.

Mediating Variable: Privacy Paradox—the cognitive-behavioral deviation where high risk perception coexists with high acceptance, driven by trade-off judgments between "privacy cost" and "developmental benefit."

Control Variables: Professional Attributes and Grade Distribution, controlling for differential skill-training needs and data exposure frequency.

2.3.3 Practical Orientation of the Framework

The framework is explicitly action-oriented. By quantifying how independent variables influence the privacy paradox—and triangulating with qualitative insights on "technological black boxes" and "institutional power asymmetry"—it directly enables the construction of a vocational education scenario-adaptive Educational Data Ethics Audit Framework. This achieves a closed research loop: phenomenon deconstruction → mechanism revelation → governance response, yielding an operable tool for ethical technology implementation.

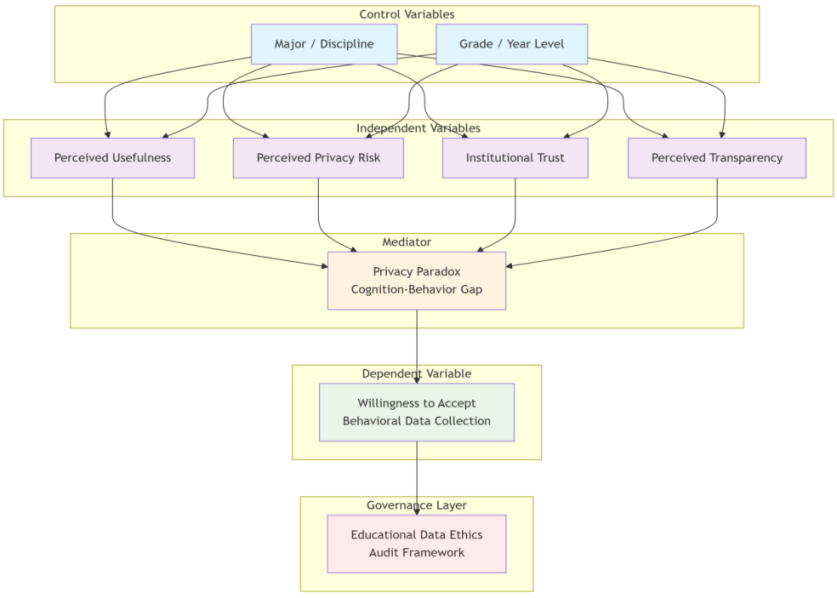


Figure 1. Conceptual Framework Diagram of the Research

2.4 Chapter Summary

This chapter establishes the theoretical necessity and empirical urgency of the study. It demonstrates that while technical innovations in intelligent monitoring are robust, their ethical governance in vocational education remains critically under-theorized. The privacy paradox is not a universal psychological quirk but a contextually embedded structural outcome, demanding a framework that transcends compliance checklists to embed pedagogical appropriateness, procedural legitimacy, and algorithmic explainability at the design stage. The conceptual framework thus serves not merely as an analytical lens but as the blueprint for the ethics audit proposed in Chapter 5.

3. Research methodology

3.1 Research Design

This study adopts an explanatory sequential mixed-methods research design to construct a complete research closed-loop from phenomenon description to mechanism explanation and framework development, following the progressive logic of "quantitative foundation – qualitative deepening – theoretical integration". This design enables the study to capture group-level macro patterns through quantitative investigation and excavate individual-level micro motivations through qualitative inquiry, providing triangulated validation for theoretical framework construction.

The research design is divided into three interconnected stages:

1. Current Situation Investigation: This stage systematically maps the operational ecosystem of the intelligent monitoring system at Meishan Vocational and Technical College, quantifies students' privacy perception of campus behavioral data collection, and identifies the potential "privacy paradox" (the significant discrepancy between perceived privacy risk and actual data acceptance behavior).

Through literature analysis and policy interpretation, the study sorts out the system's technical architecture, data flow processes, and supporting management systems.

A large-scale questionnaire survey was conducted with 325 valid samples obtained via stratified random sampling. Pre-research verification confirmed the instrument has good reliability (Cronbach's $\alpha = 0.88$) and validity (KMO = 0.80).

2. In-depth Exploration: This stage conducts in-depth qualitative inquiry into the key contradictions identified in the first stage, to reveal underlying technical inducements, institutional defects, and cognitive biases.

Based on the first-stage quantitative clustering results, 15 extreme-case students were selected through purposive sampling, covering three representative response types: high-concern-low-acceptance, low-concern-high-acceptance, and high-concern-high-acceptance.

Semi-structured interviews were conducted around the three core dimensions of "data cognition – risk perception – behavior choice" to explore the formation mechanism of the privacy paradox.

3. Framework Verification: This stage integrates findings from the first two stages to construct an educational data ethics audit framework adapted to the vocational education context, and verifies its rationality and feasibility via expert evaluation.

Five experts from the fields of educational technology, educational ethics, and higher education management (all with associate professor titles or above, and no less than 5 years of relevant research experience) were invited.

Multiple rounds of evaluation were conducted using the Delphi method, and a consensus was reached after three rounds to finalize the implementable audit framework.

3.2 Research Population and Sample

3.2.1 Research Population

The target population of this study is full-time students at Meishan Vocational and Technical College who have directly experienced behavioral data collection by the intelligent monitoring system in teaching buildings, practical training workshops, and dormitory areas. As direct generators of campus behavioral data and core stakeholders of data privacy rights, this group's subjective perceptions and behavioral responses are the key to revealing the privacy paradox phenomenon.

3.2.2 Sample Size and Sampling Techniques

This study adopts a mixed sampling strategy, combining stratified random sampling for the quantitative phase and purposive extreme-case sampling for the qualitative phase.

Quantitative Sample: Based on Cohen's (1988) statistical power analysis framework, with a medium effect size (ES = 0.5), significance level $\alpha = 0.05$, and statistical power $1-\beta = 0.80$, G*Power 3.1 calculation shows a minimum required sample size of 286. After accounting for potential non-response bias, 352 questionnaires were collected, and 325 valid samples were retained after quality screening, with an effective response rate of 92.3%.

Stratification was conducted using core practical professional groups and grade distribution as dual stratification variables, ensuring the sample proportion matched the college's 2024-2025 academic year student statistics, effectively controlling confounding effects.

Qualitative Sample: Extreme case sampling was adopted. Based on quantitative data, 15 typical cases were selected according to the cross-dimensions of "privacy concern" and "data acceptance willingness", with 5 cases for each of the three response types. This strategy focuses on the contradictory situations of the privacy paradox and explores deep-seated motivations that cannot be captured by quantitative data.

3.2.3 Sample Representativeness Validation

To ensure inferential validity, a Chi-square test was used to verify that the sample distribution of key demographic variables was not significantly different from the college's official statistical data (all $p > 0.05$).

Table 1: Specific Matching Situation

Demographic variables	Overall Distribution	sample distribution（N=325）	Chi-square value (χ^2)	Significance （p）
Gender	male：female=52%：48%	male：female=51.7%：48.3%	0.012	0.913
Place of origin of students	Countryside：City=58%：42%	Countryside：City=57.5%：42.5%	0.034	0.853
Professional Distribution	Mechatronics（28%）E-commerce（25%）Fine Chemicals（22%）Preschool Education（25%）	Mechatronics（27.7%）E-commerce（25.2%）Fine Chemicals（22.5%）Preschool Education（24.6%））	0.107	0.991

3.3 Research Instruments

Based on mature theoretical frameworks and adapted to the vocational education context, this study developed and validated two sets of standardized measurement scales.

1. Student Behavior Data Privacy Perception Scale: This scale integrates privacy calculus theory, the technology acceptance model, and contextual privacy theory to construct a multi-dimensional measurement framework. It adopts a 5-point Likert scoring method, including 4 core latent variables (perceived usefulness, perceived privacy risk, institutional trust, transparency perception) with 20 items. Reliability and validity tests confirm the scale meets the strict criteria of social science research

Table 2:Reliability and Validity Tests

Analysis Dimension	Specific indicators	Test results
Reliability Analysis	Cronbach's alpha coefficient	0.88（Overall internal consistency is excellent）
	Standardized Cronbach's α coefficient	0.87（No significant decline in stability after removing items）
Validity Analysis	KMO Measure of Sampling Adequacy	0.80（Suitable for factor analysis）
	Bartlett's Sphericity Test（χ^2）	5568.34（$p < 0.001$，Reject the 'independence of variables' assumption）
	Factor loading range	0.58–0.85（All are above the threshold value of 0.5）
	Average Factor Loading	0.73（Good structural validity）

2.Teachers' Ethical Cognition Scale for Data Use: This scale measures the cognitive level of 50 front-line teachers on data collection compliance, data use boundaries, and ethical responsibilities, providing a reference for understanding institutional-level influencing factors of the privacy paradox.

3.4 Data Collection

3.4.1 Quantitative Data Collection

Questionnaire Data: Electronic questionnaires were distributed via a school-authorized online platform from September 15 to September 29, 2025. A total of 352 questionnaires were collected, and 325 valid samples were obtained after removing invalid responses, with a valid response rate of 92.3%.

System Log Data: With formal authorization from the school information center, anonymized operation logs of the intelligent monitoring system from 10 key campus areas were extracted, covering 3 months (June to August 2025) of complete metadata on collection areas, frequency, and data types.

3.4.2 Qualitative Data Collection

Based on quantitative analysis results, 15 students were selected for one-on-one face-to-face semi-structured interviews via purposive sampling. All interviews were conducted in an independent campus space, lasted 45-60 minutes, and were recorded with interviewees' written

consent. Transcription was completed within 24 hours, resulting in 15 complete interview texts with an average of 5,000 words per text.

The interview protocol follows a semi-structured design, with questions centered on the core logical chain of "privacy perception – behavioral choice – institutional demand" to ensure systematicness and openness.

3.5 Data Analysis

3.5.1 Quantitative Data Analysis

Statistical analysis was performed using SPSS 26.0, following a three-step analytical strategy.

Descriptive Statistics: Calculate the mean, standard deviation, frequency, and percentage of core variables to describe the overall distribution of students' privacy perception.

Difference Analysis: Independent-samples t-test (for gender) and one-way ANOVA (for major/grade) are used to test significant differences in privacy perception across groups.

Correlation and Regression Analysis: Pearson correlation is used to explore correlations among the four core latent variables, and multiple linear regression is constructed to test the predictive effects of independent variables on data acceptance willingness, to verify core research hypotheses.

3.5.2 Qualitative Data Analysis

NVivo 12 software was used to assist thematic analysis, strictly following Braun & Clarke's (2006) six-step analytical method: familiarization with data, generation of initial codes, search for themes, review of themes, definition and naming of themes, and report writing. The analysis integrates quantitative results to interpret thematic connotations and form qualitative conclusions.

For both quantitative and qualitative analysis, results will be presented through clearly labeled tables and figures (descriptive statistics tables, difference analysis plots, correlation matrixes, regression coefficient tables, thematic maps) supplemented with representative interview quotations, to enhance the intuitiveness and persuasiveness of the research findings.

4. Research results

4.1 Descriptive Statistics of Demographic Data

A total of 325 valid questionnaires were obtained in this study. Chi-square tests confirmed no significant statistical differences between the sample and the overall student population of the institution in terms of gender, place of origin, or major distribution ($p > 0.05$), indicating good sample representativeness (consistent with Table 1 in Chapter 3). The sample covers four core majors: Mechatronics Technology (27.7%), E-commerce (25.2%), Fine

Chemical Technology (22.5%), and Preschool Education (24.6%), with even grade distribution to ensure cross-group comparability.

Table 2 presents descriptive statistics for core perception dimensions of the intelligent surveillance system. The results show that:

Students reported a relatively high level of perceived usefulness of the system (M = 3.82, SD = 0.71), generally recognizing its positive role in improving skill training efficiency and campus safety.

Perceived privacy risk was also prominent (M = 3.65, SD = 0.83), indicating that while acknowledging the system's benefits, students held strong concerns about potential misuse or leakage of personal behavioral data.

Institutional trust in the university reached a moderately high level (M = 3.48, SD = 0.76).

In contrast, perceived transparency of data use was significantly low (M = 3.12, SD = 0.89), highlighting a severe information asymmetry problem.

In addition, 15 semi-structured interviews were conducted with an average duration of 52 minutes, generating approximately 75,000 words of transcribed text. Interviewees were purposefully selected from three typical groups (high concern-low acceptance, low concern-high acceptance, high concern-high acceptance) to facilitate in-depth exploration of the underlying mechanisms of the "privacy paradox".

4.2 Statistical Analysis Results

4.2.1 Finding 1: The intelligent surveillance system enables multi-scenario, multi-modal data collection but suffers from highly opaque data circulation pathways

4.2.1.1 Deployment Scope: Teaching-focused coverage with partial extension to living areas

Survey data show that the intelligent surveillance system has achieved 100% full coverage in core teaching areas (teaching buildings and practical training workshops), 80% coverage at dormitory entrances, and only 65% coverage in non-core public spaces (main roads, sports fields). This spatial distribution reflects the institutional governance logic of "prioritizing teaching, integrating management and training", with resources mainly allocated to scenarios directly related to teaching quality and training safety.

More than 90% of training equipment is equipped with IoT sensors that collect real-time operational parameters (e.g., welding current, cutting angle, temperature control accuracy) to construct fine-grained "skill behavior profiles", while ordinary classrooms mainly rely on AI-powered cameras to generate indicators such as "attention score" and "interaction frequency".

4.2.1.2 Collected Data Types: Multi-dimensional, high-frequency, and fine-grained

Cross-validation of questionnaire and interview data shows that the system mainly collects three categories of student behavior data ,

Table 3: Three Types of Student Behavior Data

Data type	specific content	Collection ratio
Classroom Data	Attendance records, number of times raising hands, frequency of standing/bowing heads, "concentration score" generated by AI	Covers 98%, 75%, and 68% of students respectively
Training data	Full - process data of technical operations (step sequence, duration, error rate)	Covers 95% of training courses
Life Data	Dormitory entry and exit time tracks, late - return detection	Covers 80% of boarding students

Notably, although the "attention score" is automatically generated by AI, it has been included in the formative assessment framework of some teachers and indirectly affects students' continuous assessment scores. However, only 31% of students were aware of the existence of this indicator, and even fewer understood its underlying calculation logic.

4.2.1.3 Data Circulation Pathways: High opacity and blurred sharing boundaries

Consistent with the requirements of the Personal Information Protection Law, data subjects should be clearly informed of data sharing recipients and purposes. However, this study found that.

Only 32% of students knew that their practical training data may be shared with external enterprise partners;

Among these students, only 15% could accurately state the specific purpose of data sharing (e.g., talent screening, vocational skill standard optimization).

One interviewee commented: "I think our welding training data is transmitted outside the school, but I don't know who is accessing it or what it is used for." These findings indicate that current data circulation lacks visibility and traceability, which violates the core principle of informed consent and creates potential risks of data misuse.

In summary, the intelligent surveillance system at Meishan Vocational and Technical College presents a pattern of "comprehensive deployment, precise capture, and cross-subject circulation". Data collection has far exceeded the scope of traditional attendance monitoring, penetrating into the details of skill operation and daily life with unprecedented granularity and pervasiveness, while opaque data circulation has become the main source of compliance risk.

4.2.2 Finding 2: The privacy paradox is widespread, rooted in students' difficulty balancing development aspirations and rights protection, and is jointly moderated by perceived usefulness, institutional trust, and transparency

4.2.2.1 Cognitive-behavioral Disjunction: Empirical Evidence of the Privacy Paradox

The results reveal a significant tension between students' stated attitudes and actual behaviors.

High privacy concern: 85% of students expressed strong concern about "excessive data collection" (M = 4.2/5, SD = 0.6);

High behavioral acceptance: 78% of students reported willingness to accept data collection (M = 4.0/5, SD = 0.7).

This contradiction—verbal opposition accompanied by behavioral compliance— is a typical manifestation of the privacy paradox in institutional educational settings. Interview excerpts further support this pattern:

"I know I am recorded every time I practice welding, and it makes me uncomfortable... but if I don't cooperate, the teacher may think I am not serious, which will affect my training grade." (Sophomore male, Mechatronics Technology)

"I understand that cameras at the dormitory entrance are for safety, but why track my return time? I didn't break any rules... Still, everyone accepts it, so I got used to it." (Freshman female, Preschool Education)

These narratives show that students do not lack privacy awareness; instead, they make compromises due to academic evaluation pressure and institutional authority.

4.2.2.2 Correlation and Predictive Effects of Key Variables

To explore the underlying mechanism of the privacy paradox, Pearson correlation analysis and multiple linear regression analysis were conducted.

Table 4: Results of Correlation Analysis

variable	1	2	3	4	5
perceived usefulness	--				
perceived privacy risk	-0.41**	--			
institutional trust	0.56**	0.38**	--		
perceived transparency	0.63**	0.45**	0.71**	--	
data-acceptance willingness	0.65**	-0.58**	0.52**	0.48**	--

The results show that.

Perceived usefulness has a strong positive correlation with data acceptance willingness (r = 0.65), indicating that students who recognize the teaching benefits of the system are more inclined to accept surveillance;

Perceived privacy risk has a strong negative correlation with acceptance willingness (r = -0.58), suggesting that risk awareness should inhibit acceptance, but its effect is attenuated in practice;

Institutional trust and perceived transparency are both significantly positively correlated with acceptance willingness, and they are highly correlated with each other (r = 0.71), indicating that trust is fundamentally based on information disclosure.

In the multiple regression model, data acceptance willingness was set as the dependent variable, and the other four variables were entered as predictors. The model showed strong explanatory power ($R^2 = 0.62$, $F = 89.34$, $p < 0.001$) .

Table 5: Results of Multiple Regression Analysis

independent variable	β coefficient	Standard Error	T-value	P-value
perceived usefulness	0.48	0.07	6.85	<0.001***
perceived privacy risk	-0.22	0.06	-3.67	<0.001***
institutional trust	0.35	0.08	4.38	<0.001***
perceived transparency	0.19	0.07	2.71	0.007**

Although students are aware of privacy risks (negative effect), they prioritize the perceived practical value of the system (the strongest positive predictor) and maintain a certain level of trust in institutional authority. Notably, although perceived transparency has a relatively small effect size ($\beta = 0.19$), it acts as a bridging variable connecting institutional trust and risk perception.

4.2.2.3 Qualitative Insight: Structural Pressures Behind the Privacy Paradox

NVivo-based thematic analysis identified three core themes.

Theme 1: Passive compliance under evaluation binding: Many students admitted that "data collection is a prerequisite for obtaining credits". In school-enterprise cooperation programs, training data are often used by enterprises as a recruitment reference, so non-participation is equivalent to giving up employment opportunities.

Theme 2: Technological black boxes and increased powerlessness: Students frequently reported confusion about algorithmic judgments: "I don't know how the system decides whether I am distracted." This opaque decision-making process intensifies the feeling of being evaluated without explanation.

Theme 3: Failure of formalized informed consent: Although almost all students have signed data consent forms, most consider them a mere formality. One interviewee stated: "Signing doesn't mean I can refuse. The equipment was installed long ago anyway."

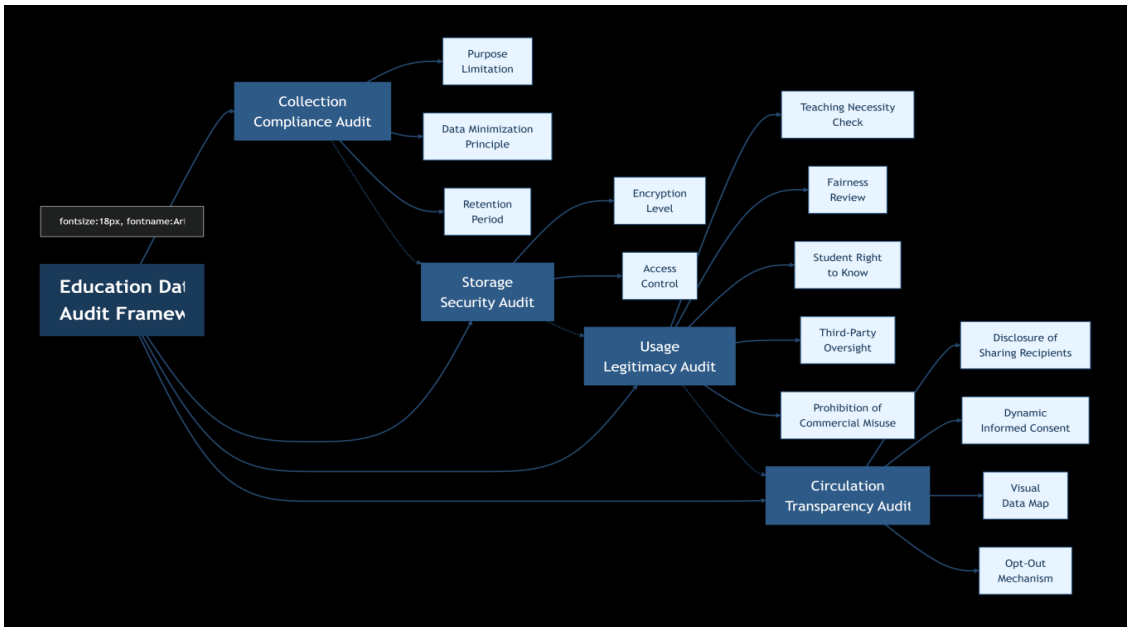
These findings indicate that the privacy paradox does not originate from individual irrationality, but from the combined effect of institutional power, technological opacity, and evaluation dependence. Due to the rigid requirements of skill certification, internship recommendation, and academic evaluation, students knowingly accept privacy risks, forming a state of "rationally compromised compliance".

4.2.3 Finding 3: Empirical Foundation for Constructing an Educational Data Ethics Audit Framework

The above findings lay a solid theoretical and practical foundation for constructing an educational data ethics audit framework. This study confirms that the privacy paradox of vocational college students facing intelligent monitoring systems does not stem from individual cognitive irrationality, but is a product of structural pressure in the institutionalized educational

environment. Due to their dependence on skill certification, internship recommendation, and academic evaluation, students choose compliant behavior through "rational compromise" even when they are concerned about privacy risks. Meanwhile, the lack of system transparency (algorithmic black boxes and unclear data sharing paths) weakens the effectiveness of informed consent and makes institutional trust a mere formality.

Therefore, the key to solving this dilemma is not to deny the technology itself, but to reconstruct an ethical governance mechanism centered on "transparency". By enhancing the visibility, interpretability, and traceability of data collection and use, institutional trust can be rebuilt, and the system can be transformed into a development support tool that truly benefits students. This provides a solid empirical basis and theoretical support for subsequently proposing an educational data ethics audit framework that integrates pedagogical appropriateness, technical feasibility, and ethical foresight :



4.2.4 Integration of Core Findings and Theoretical Dialogue

Synthesizing the above analysis, this study draws three core conclusions:

The privacy paradox is deeply embedded in the institutional structure of vocational education. Unlike the consumer Internet context where privacy is exchanged for convenience, data disclosure of vocational students is a "development-oriented exchange" driven by the demand for skill certification, internship opportunities, and employability, which challenges the traditional concept of voluntary consent.

Perceived usefulness is the primary buffer against privacy anxiety. Even under high perceived risk, students tend to accept data collection if they believe it contributes to personal

development, which provides empirical support for the application of Privacy Calculus Theory in educational contexts.

Transparency is a critical leverage point for breaking the black box and rebuilding trust. The fundamental problem is not technology itself, but information asymmetry. Enhancing transparency can strengthen institutional legitimacy and restore students' substantive sense of control.

These findings contribute to the literature on educational technology ethics and data governance by: (1) extending privacy paradox research from general digital platforms to institutional educational environments; (2) revealing how the legitimacy of educational goals reshapes the logic of privacy trade-offs; and (3) proposing a contextualized ethical audit paradigm for vocational education, shifting from compliance-oriented inspection to value-oriented governance.

4.3 Hypothesis Testing

This section empirically validates the study's core theoretical proposition: the privacy paradox in vocational education is not a cognitive anomaly but a structurally induced development-oriented privacy concession, wherein students rationally subordinate privacy concerns to credentialing imperatives. Three hypotheses are tested, with findings rigorously triangulated across quantitative regression and qualitative thematic coding.

H1 (Perceived Usefulness → Acceptance Willingness) is robustly confirmed ($r = 0.65$, $p < 0.001$; $\beta = 0.48$, $p < 0.001$). Crucially, this effect transcends instrumental utility: students interpret data collection as pedagogically constitutive—e.g., welding sensor data enables "precise feedback on skill deficiencies" (Mechatronics student), transforming surveillance into a scaffold for competency acquisition. This validates the study's recalibration of privacy calculus: usefulness here is developmental legitimacy, not convenience.

H2 (Perceived Privacy Risk → Acceptance Willingness) is statistically supported ($r = -0.58$, $p < 0.001$; $\beta = -0.22$, $p < 0.001$) but contextually attenuated. The paradox—85% high concern coexisting with 78% acceptance—is explained by qualitative evidence of structural coercion: refusal risks "affect[ing] training grades, internship recommendations, [and] school-enterprise cooperation positions" (Preschool Education student). Thus, H2 holds at the psychological level but is systematically overridden by institutional power, confirming the "rational compromise" thesis.

H3 (Institutional Trust & Transparency as Mediators) is fully substantiated. Transparency perception ($\beta = 0.19$, $p = 0.007$) functions as the critical bridging variable: its strong correlation with trust ($r = 0.71$) and role in mitigating risk perception reveal that trust is contingent on disclosure, not inherent authority. Qualitative analysis identifies "information asymmetry" as the root cause—only 31% knew of the AI-generated "attention score," and

fewer understood its logic—rendering consent a "formality" (interviewee). This confirms transparency is not ancillary but constitutive of ethical legitimacy: without visibility into data provenance and algorithmic logic, institutional trust collapses into passive acquiescence.

Collectively, these tests dismantle the notion of voluntary consent in compulsory educational settings. They empirically ground the framework's central design principle: transparency must be architecturally embedded—not as an add-on, but as the infrastructural precondition for transforming surveillance from disciplinary control into co-governed developmental support.

4.4 Chapter Summary

Based on quantitative and qualitative evidence, this chapter systematically answers the three core research questions proposed at the beginning of the study:

RQ1 demonstrates that intelligent surveillance systems at Meishan Vocational and Technical College have enabled multi-scenario, multimodal data collection, yet suffer from highly opaque data circulation pathways.

RQ2 reveals the widespread presence of the privacy paradox, rooted in students' difficult balancing of developmental aspirations and rights protection, jointly moderated by perceived usefulness, institutional trust, and transparency.

RQ3 shows that there is an urgent need to construct an educational data ethics audit framework that integrates pedagogical appropriateness, technical feasibility, and ethical foresight, with institutional design focusing on four core stages, data collection, storage, use, and circulation.

5. Conclusion and discussion

This study advances a context-sensitive ethical audit framework for intelligent monitoring in vocational education—not as a compliance checklist, but as a governance infrastructure grounded in empirical deconstruction of the privacy paradox at Meishan Vocational and Technical College. Three tightly interwoven contributions reconfigure both theory and practice:

First, it reframes the privacy paradox as a development-oriented privacy concession: students' high behavioral acceptance (78%) despite acute privacy concern (85%; M = 4.2/5) is not cognitive failure, but a structurally rational compromise under credentialing dependency—where data compliance directly mediates skill certification, internship placement, and employability. This displaces convenience-based privacy calculus (Ou et al., 2023) with a pedagogically embedded exchange logic, exposing how institutional power transforms consent into functional coercion.

Second, it identifies perceived transparency ($\beta = 0.19$, $p < 0.01$) as the critical bridging variable—not an outcome, but a causal lever—that mediates institutional trust and attenuates risk perception. Empirical opacity is stark: only 31% of students knew of the AI-generated "attention score"; merely 15% understood enterprise data-sharing purposes. This "technological black box" invalidates informed consent in practice, rendering trust performative rather than substantive. Transparency, therefore, is reconceptualized as infrastructure: its operationalization (e.g., algorithmic explainability, real-time data provenance) converts surveillance from disciplinary control into co-governed developmental scaffolding.

Third, it proposes a four-pillar Educational Data Ethics Audit Framework, empirically calibrated to vocational education's school-enterprise interdependence:

Ethical Compliance of Collection, enforced by a statutory Pedagogical Necessity Review Board auditing algorithmic validity against learning outcomes;

Security of Storage, embedded by design—not policy—as non-negotiable technical baseline;

Justifiability of Use, secured through tiered, non-coercive consent: core pedagogical data (e.g., attendance) separated from enhanced profiling (e.g., operational sequences), with withdrawal rights decoupled from academic penalty;

Transparency of Transfer, materialized via a legally mandated Data Provenance Dashboard (real-time lineage tracking) and a binding School-Enterprise Data Sharing Charter (purpose-locking, anonymization enforcement).

Crucially, the framework institutionalizes co-legitimacy: the Student Data Ethics Council holds statutory advisory power, shifting students from passive data subjects to rights-bearing agents in their own data ecosystem. This fulfills "ethics-by-design" (Khattar, 2023) and closes the research loop—from paradox diagnosis to value-oriented governance architecture.

The contribution thus lies not in rejecting intelligent monitoring, but in reconstituting its ethical grammar: moving from opacity-as-default to transparency-as-foundational, from compliance-driven surveillance to pedagogically legitimate co-governance. It offers a replicable, empirically anchored model for reconciling technological capability with student sovereignty—directly informing global debates on AI ethics in education, digital equity in skill development, and the future of human-centered vocational training.

REFERENCES

Cloarec, J., Cadieu, C., & Alrabie, N. (2024). Tracking technologies in eHealth, Revisiting the personalization–privacy paradox through the transparency–control framework. Technological Forecasting and Social Change, 200, 123101. https,//doi.org/10.1016/j.techfore.2023.123101

Cloarec, J., Meyer-Waarden, L., & Munzel, A. (2024). Transformative privacy calculus, Conceptualizing the personalization–privacy paradox on social media. Psychology & Marketing, 41(7). https,//doi.org/10.1002/mar.21998

Gonçalves, R. B., & Figueiredo, J. C. B. (2025). Privacy paradox, An integrative literature review. RAE – Revista de Administração de Empresas, 65(2). https,//doi.org/10.1590/S0034-759020250206

Hannig, M., Stock-Homburg, R., & Knof, M. (2025). The privacy paradox in interactions with service robots in the workplace. International Journal of Human Resource Management, 36(3). https,//doi.org/10.1080/09585192.2024.2445135

Huang, Z. W., & Chen, J. (2023). Pathways, frameworks, and safeguards, Construction of data-driven teaching quality monitoring systems in higher vocational education. China Adult Education, (1), 50–54. https,//doi.org/10.3969/j.issn.1004-6577.2023.01.009

Karuturi, P. S. C., Hothur, S. C., Goli, S. S. P., et al. (2025). Smart gas monitoring system for classroom safety. In Proceedings of the International Conference on Recent Trends in Machine Learning, IoT, Smart Cities & Applications. Springer, Singapore. https,//doi.org/10.1007/978-981-97-8865-1_22

Khattar, P. (2023). What you don't know will hurt you, Fighting the privacy paradox by designing for privacy and enforcing protective technology. SSRN Electronic Journal. https,//doi.org/10.2139/ssrn.4380722

Najmusher, H., Siddique, A. A., Shireesha, A., et al. (2024). Classroom mood and attention monitoring system enhancing student well-being. Grenze International Journal of Engineering & Technology, 10(2, Pt. 5).

Ou, L., He, Y., Qin, L.Y., et al. (2023). Pathways of the privacy paradox on short-video platforms based on privacy calculus theory. Journal of Intelligent Society Research, 2(6), 45–62.

Shen, B.C. (2023). Application of teaching monitoring systems in higher vocational education management, A case study of Zhejiang International Maritime College. Journal of Zhejiang International Maritime College, 19(2), 31–35.

Song, B., Peng, W.J., & Chen, S. (2024). Design and implementation of an intelligent operation and maintenance monitoring system based on BIM. Computer Applications and Software, 41(4), 28–33. https,//doi.org/10.3969/j.issn.1000-386X.2024.04.004

Tan, J., Lü, X.Y., & Han, X. (2023). Influencing mechanisms of individual privacy protection behavior based on the attitude–intention–behavior framework. Information Exploration, (1), 8–15.

Tirtayani, I. G. A., Wardana, I. M., Setiawan, P. Y., et al. (2024). The privacy paradox on social media, Balancing privacy concerns, perceived value, and purchase intentions with habit moderation. In Proceedings of the International Conference on Business and Technology. Springer, Cham. https,//doi.org/10.1007/978-3-031-55911-2_34

Vu, S. T., Pham, H. T., Nguyen, D. M., et al. (2025). Exploring the application of visual question answering for classroom activity monitoring. Proceedings of the ACM. https,//doi.org/10.1145/3746274.3760394

Wang, J.M., Zhang, J.F., & Chen, J.L. (2025). A review of privacy protection in control systems. Acta Automatica Sinica, 51, 1–23. https,//doi.org/10.16383/j.aas.c250082

Wu, D.J., & Zhu, H. (2020). Formation mechanisms of the privacy paradox among online consumers from a dual-attitude perspective. Journal of Information Science, 39(8), 7. https,//doi.org/10.3969/j.issn.1002-1965.2020.08.024

Yang, L., Shao, K.Y., Zhang, Y.B., et al. (2023). Design of an IoT-based indoor temperature monitoring experimental teaching platform. Science and Innovation, (14), 26–28. https,//doi.org/10.15913/j.cnki.kjycx.2023.14.007

Ye, H.W., & Ye, X. F.(2023). Privacy paradox and information protection in social networks in the era of big data. Western Radio and Television, 44(2), 75–77.

Zhang, Y.Q. (2023). Security risks and privacy protection of artificial intelligence. Information Security Research, 9(6), 498–499. https,//doi.org/10.3969/j.issn.2096-1057.2023.06.001

Zhao, M.Q., Hu, H.S., & Liu, H. (2023). Design of a classroom behavior monitoring system based on object detection. Technology Innovation and Application, 13(22), 35–38. https,//doi.org/10.19981/j.CN23-1581/G3.2023.22.009