Journal of Information, Communication and Ethics in Society

Examining students' perception of surveillance technology and its impact on privacy in educational institutions

Oluwole Olumide Durodolu
Department of Information Science, University of South Africa, Pretoria, South Africa

Agnes Joe Shaibu and Victor Olusegun Babatunde
Department of Mass Communication, Kwara State University, Malete, Nigeria, and

Shakirat Ronke Yusuff
Department of Computer Science, Kwara State University, Malete, Nigeria

Received 5 October 2025
Revised 18 December 2025
Accepted 28 January 2026

Abstract

Purpose – The ubiquity of digital surveillance technologies is at the forefront of debates on balancing collective security while ensuring individual privacy. Ethical concerns of individual privacy, freedom and misuse are at the crux of ongoing global discourse, with the integration of artificial intelligence into surveillance further increasing the intrusive nature of these technologies. This study examined students' perception of surveillance technology and its impact on privacy. Questions articulated from the problematic bordered around the level of awareness, perception on the impact of surveillance technology, attitude towards surveillance and beliefs in the regulation of surveillance in educational institutions among others.

Design/methodology/approach – This study was premised on the pragmatic paradigm involving the integration of both quantitative and qualitative approaches. Data were collected from 450 respondents using a structured questionnaire.

Findings – Findings revealed a significant association between students' awareness of surveillance technologies and their frequency of observing them on campus ($\chi^2 = 47.80$, $df = 6$, $p < 0.001$; mixed perceptions of privacy with most respondents (54.9%) feeling their privacy was moderately respected, a notable minority expressing concern over inadequate protection, and nearly a quarter (24.2%) reporting behavioural changes due to being watched; and a statistically significant positive relationship between trust in institutional data handling and confidence in data protection ($\rho = 0.144$, $p < 0.01$).The qualitative responses revealed that students acknowledged the usefulness of surveillance for safety, but insisted on clear boundaries regarding scope, usage and access. This study concluded that surveillance in education was a double-edged phenomenon that enhances safety and order but raised several challenges that called for deliberate governance strategies. It was recommended that educational institutions developed clear communication strategies on the use of surveillance technologies and accompany such with privacy protection policies.

Originality/value – The findings contribute to academic debates on digital ethics, governance and the balance between security and privacy in learning environments, while offering actionable recommendations

© Oluwole Olumide Durodolu, Agnes Joe Shaibu, Victor Olusegun Babatunde and Shakirat Ronke Yusuff. Published by Emerald Publishing Limited. This article is published under the Creative Commons Attribution (CC BY 4.0) licence. Anyone may reproduce, distribute, translate and create derivative works of this article (for both commercial and non-commercial purposes), subject to full attribution to the original publication and authors. The full terms of this licence may be seen at http://creativecommons.org/licences/by/4.0/

Journal of Information, Communication and Ethics in Society
Emerald Publishing Limited
1477-996X
DOI 10.1108/JICES-10-2025-0279

Downloaded from http://www.emerald.com/jices/article-pdf/doi/10.1108/JICES-10-2025-0279/11507623/jices-10-2025-0279en.pdf by guest on 10

for institutions to design communication strategies and privacy policies that safeguard both safety and individual rights.

Keywords Surveillance technology, Privacy, CCTV, Security, Personal information, Unauthorised access

Paper type Research paper

Introduction

In recent years, the rapid and sustained proliferation of digital surveillance technologies has led to strong debate and intense deliberation globally over how to ensure balance in the collective security of lives and property with the protection of individual privacy. Governments, private corporations and educational institutions are gradually relying on these systems to track behaviour, gather sensitive data and anticipate threats. It is generally agreed that such measures are often justified because of the importance of human safety. But they have, at the same time, raised weighty ethical and legal concerns by eroding and sabotaging personal privacy rights (Saputra and Handayani, 2024).

Surveillance technologies infrastructure is a vital component of modern society that is pervading several aspects of personal and public life. Especially, in the view of Wheatley (2024), the deployment of cutting-edge surveillance facilities, from the prevalent Closed-Circuit Television (CCTV) networks to sophisticated digital tracking devices, reflects a momentous technological growth designed to enhance security procedures and monitor various activities. Still, the ever presence of these technologies has raised a critical ethical question about privacy, individual freedom and the possibilities of misuse (Wheatley, 2024),

The incorporation of Artificial Intelligence (AI) has further transformed and complicated the surveillance landscape, making it more prevailing and intrusive. AI-driven systems, most especially those powered by machine learning, are proficient in processing enormous torrents of everyday data to detect, analyse and even envisage human actions in real time (Fontes *et al.*, 2022). This has led to a substantial global investment in AI-enabled surveillance systems, with facial recognition technology (FRT) emerging as a leading tool (Nunn, 2001). By mapping and authenticating individuals through facial features, this FRT also allows institutional authorities to conduct prompt identification across wide geographical area, from policing and immigration control to the airport security checkpoints. Nevertheless, the growing deployment of FRT exemplifies the Janus-faced nature of surveillance technologies: while improving efficiency and safety, they at the same time deepen growing concerns about privacy, civil liberties and the normalisation of persistent monitoring (Lai and Rau, 2021).

Building on the perceptions of Saputra and Handayani (2024), the issue of privacy is understood as a fundamental human right that has been upheld by prominent international organisations like the United Nations. Yet, digital surveillance poses a grave danger to this important right by allowing the tracking of people's movements, the monitoring of their communications and the massive collection of personal data. Indications from current studies have suggested that when surveillance becomes extreme, it destabilises public trust and often creates a "chilling effect," in which individuals conceal their behaviour because of the fear of monitoring. Authors like Saputra and Handayani (2024) and Lee, *et al.* (2012) further stress that surveillance raises weighty ethical questions tied to consent, autonomy and fairness. Another vital issue is the absence of transparency, especially because most people remain uninformed about how extensively their personal data is gathered and used. In addition, the danger of biased surveillance systems has heightened genuine concerns, since such biases can reinforce discriminatory practices against category of people who are

Downloaded from http://www.emerald.com/jices/article-pdf/doi/10.1108/JICES-10-2025-0279/11507623/jices-10-2025-0279en.pdf by guest on 10

marginalised. Therefore, the question is: what is the perception of students on surveillance technology and what is its impact on privacy in educational institutions?

Theoretical foundation

The Unified Theory of Acceptance and Use of Technology (UTAUT) propose an inclusive framework for understanding students' perceptions of surveillance technologies in educational institutions by elucidating how acceptance, resistance and privacy concerns are socially and institutionally constructed (Bayaga and du Plessis, 2024). Within this theoretical framework, performance expectancy shapes acceptance to the extent that students perceive surveillance technologies as enhancing safety, academic integrity or learning outcomes. However, when benefits appear institution-centred rather than student-centred, scepticism and resistance increase. Effort expectancy, particularly the invisible or low-interaction nature of surveillance systems, may facilitate acceptance while simultaneously normalising monitoring practices and obscuring underlying privacy intrusions (Ilci, 2020).

Social influence highlights the role of institutional authority and peer norms in compelling compliance, revealing asymmetrical power relations in which acceptance often reflects obligation rather than consent (Khan, *et al.*, 2024). Facilitating conditions extend beyond technical infrastructure to include governance mechanisms such as transparency, data protection and accountability. However, deficiencies in these areas intensify privacy concerns and erode trust (Sarifudin and Damanik, 2024). Furthermore, moderating variables, including age, experience and voluntariness, help explain differential privacy perceptions, with digitally literate students often exhibiting heightened awareness of data misuse and involuntary participation amplifying feelings of coercion. (Martin and Shilton, 2016).

Importantly, applying UTAUT to surveillance contexts necessitates the integration of privacy as a critical mediating variable, as behavioural acceptance does not necessarily imply ethical legitimacy (Reith, *et al.*, 2020). Generally, the framework reframes surveillance adoption in educational institutions as a contested socio-technical process shaped by power, governance and privacy ethics, rather than a neutral outcome of perceived usefulness or ease of use (Venkatesh *et al.*, 2003).

Research questions

RQ1. What is the level of awareness among students regarding the use of surveillance technologies in their institution?

RQ2. How do students perceive the impact of surveillance technologies on their personal privacy?

RQ3. How do demographic characteristics influence perceptions of students on surveillance technology and its impact on privacy?

RQ4. Is there a relationship between the level of awareness of surveillance technologies and the frequency with which students notice them in their academic life?

RQ5. Do students' attitudes towards surveillance (e.g. trust, consent, transparency) influence their level of comfort with being monitored?

RQ6. Is there a significant relationship between students' perception of institutional data responsibility and their confidence in data protection?

RQ7. Do students believe that surveillance in educational institutions should be regulated by policies that involve student input?

Downloaded from http://www.emerald.com/jices/article-pdf/doi/10.1108/JICES-10-2025-0279/11507623/jices-10-2025-0279en.pdf by guest on 10

Hypothesis

H1. There is a significant awareness among students about surveillance technologies used in their institution.

H2. There is a significant relationship between students' awareness and their reported frequency of noticing surveillance technologies.

H3. Students perceive surveillance technologies as having a significant impact on their personal privacy.

H3. Students' attitudes towards surveillance significantly influence their level of comfort with being monitored.

H4. There is a significant relationship between students' trust in institutional data handling and their confidence in data not being misused.

H5. Students significantly support policy regulation of surveillance involving student input.

Literature review

Surveillance system has recently become a pivotal instrument in crime prevention and investigation. This is because it accelerates evidence gathering and facilitates prosecution, most especially in tackling organised and serious crimes. For instance, in many developed societies, electronic surveillance is no longer an exceptional activity but routine, which is embedded through visible, concealed or semi-obscured cameras and sensors that pervade both public and private environments (Odoemelam, 2015). Even though legal frameworks are designed to regulate the use of surveillance technology like CCTV in public arenas, its use and application range beyond state security to domestic, official spaces and community locations, where it also functions as a device for social control. Parental monitoring of children, managers' oversight of employees and governments' scrutiny of citizens have blurred the line between protection and coercion.

We begin by outlining the concept of surveillance state, which is increasingly facilitated by pervasive sensors, cloud computing infrastructures and the ubiquitous artificial intelligence systems designed for pattern recognition and behavioural prediction. We then provide a concise characterisation of four key surveillance technologies that are gaining traction within PreK–12 schools, universities, educational research and technology design:

- location tracking;
- facial recognition;
- automated speech recognition; and
- social media data mining (Niemi *et al.*, 2023).

In recent years, facial recognition technology (FRT) has become one of the commonly discussed and debated uses of artificial intelligence. It is seen as a double-edged tool; on one hand, it improves efficiency, security and automation, but on the other hand, it raises serious ethical, legal and human rights concerns (Shao *et al.*, 2021). FRT works by identifying and verifying people through their facial features captured in photos or videos, and it has quickly moved from experimental labs into everyday use in social, commercial and institutional settings (Mantello *et al.*, 2023).

Downloaded from http://www.emerald.com/jices/article-pdf/doi/10.1108/JICES-10-2025-0279/11507623/jices-10-2025-0279en.pdf by guest on 10

Another significant strand of the literature focuses on algorithmic bias and discrimination. Empirical studies have demonstrated that many FRT systems exhibit higher error rates when identifying women, ethnic minorities and younger or older populations, thereby reproducing and amplifying existing social inequalities (Shao *et al.*, 2021). Such biases raise serious ethical concerns, particularly when FRT is deployed in high-stakes environments such as policing, education or immigration control, where misidentification can result in material harm.

The debate over surveillance technology is far from settled. Governance in the digital age is increasingly dependent on constant information flows, and these techniques of monitoring people have enabled unhindered access, frequently intruding upon privacy (Fernando *et al.*, 2025). These debates have echoed prior philosophical discourses on the Panopticon and the disciplinary "gaze," concepts that have become emblematic of modern systems of governance. What is significant about the present epoch, however, is the merging of technological, commercial and policy dynamics, which has amplified the pervasiveness of surveillance and raised persistent questions concerning its long-term implications. Rather than diminishing in its importance, this convergence also shows the urgent need for deeper inquiry into how surveillance technology is reshaping the boundaries of governance and privacy (Fernando *et al.*, 2025).

At the mechanical level, surveillance technologies rely somewhat on the processes of observation, tracking, documentation and analysis, which are supported by advanced information systems. Devices like cameras and sensors gather environmental and behavioural data, which are carefully stored locally or by means of cloud-based set-ups, and conveyed through wired and wireless networks relayed to control centres for processing (Nayyar, Nguyen, and Nguyen, 2019). Technologies like this not only expand the reach of surveillance but also strengthen the growing entanglement of governance, security and digital infrastructures in contemporary society.

Significance of the study

This research is imperative because it offers practical and policy understandings of how students observe surveillance technologies in the university environment. It affords university authority with direction on how to balance institutional security with respect to student freedom, although stressing the importance of digital citizenship and privacy awareness training. At the strategic policy level, the findings of this study can enlighten institutional and national regulations that defend privacy rights and at the same time, ensure that surveillance practices are done in an ethical, legitimate and proportionate manner.

In terms of theoretical implications, the research extends the existing deliberations on privacy and surveillance by revealing how important concepts like the privacy calculus and panopticons play out in the educational environment. It likewise fills an existing gap in the extant literature. This is because research in surveillance technology is usually fixated on workplaces, social media or public spaces, except in the school environment, which is underexplored. As a result of this, students' experiences are left out. The research contributes to and gives renewed perspectives that link education with surveillance and information ethics, at the same time providing a foundation basis for future research in this area.

Methodology

This study used both qualitative and quantitative methods, guided by a pragmatic philosophical paradigm. This paradigm offers the epistemological flexibility necessary to address complex social and behavioural phenomena comprehensively, because it supports the integration of both quantitative and qualitative approaches. In this case, the quantitative

Downloaded from http://www.emerald.com/jices/article-pdf/doi/10.1108/JICES-10-2025-0279/11507623/jices-10-2025-0279en.pdf by guest on 10

component, guided by post-positivism, enabled hypothesis testing through statistical analysis, while the qualitative component, informed by interpretivism, allowed exploration of participants' perceptions. Therefore, the pragmatist approach provides a comprehensive philosophical foundation for the mixed methods design adopted. Since the student population for this research is relatively homogeneous that is (similar in age group, educational exposure and institutional environment), this means the level of inconsistency among students is low. The implications are that this smaller sample can still reliably represent the larger population. In this case, statistical sampling theory suggests that once a sample reaches around 384 respondents, it is acceptable to generalise findings to a large population (at a 95% confidence level with ± 5% margin of error).

In this study, a questionnaire was used as an instrument of data collection. The questionnaire systematically collected students' demographic profiles, awareness, perceptions and attitudes towards surveillance technologies, while assessing their perceived impact on privacy and eliciting recommendations for ethical and transparent surveillance practices in educational institutions. The questionnaire adopted a mixed-methods design, combining structured (closed-ended) items with open-ended questions. Consequently, data analysis proceeded through two complementary analytical strands: quantitative statistical analysis and qualitative thematic analysis, followed by integration at the interpretive stage. Through combined statistical analysis, systematic coding and thematic saturation, this questionnaire enables **a** robust, empirically grounded examination of student perceptions of surveillance technologies and their implications for privacy, autonomy and institutional trust in educational environments.

The study adopted a non-probability sampling technique, specifically voluntary response sampling. Although the questionnaire was distributed to the entire population of students in the University, only 450 students voluntarily responded. Consequently, the sample reflects self-selected participants rather than a randomly drawn sample. Therefore, with 450 responses, the study not only meets but exceeds this threshold, making the sample statistically sufficient to reflect the opinions of 20,000 students. Using a sample size of 450 in a population of 20,000 has yielded a confidence level of about 95% and a margin of error close to 4.6%, which falls within the acceptable standards for social science research. Reliability of the instrument used for this research was assessed using Cronbach's alpha, and the result yielded a coefficient of 0.84, which indicated that the instrument is highly consistent and justifies that the scale is reliable.

Results and interpretation

As shown in Table 1, most respondents (65.6%) were between the ages of 18 and 22 years, indicating that most participants were typical university-age students. A notable 23.6% were under 18, while only 11% were aged 23 years or older.

Furthermore, in terms of gender, more females (60.7%) than males (39.3%) participated in the study, suggesting greater female representation in the sample. Regarding the level of study, a large proportion (78.0%) were pursuing a bachelor's degree, while 21.3% were enrolled in diploma, ND or NCE programmes. Postgraduate students made up less than 1% of the total sample.

However, from Table 1, the study shows that the faculty representation was heavily skewed towards Mass Communication (91.3%), with only 8.7% from the Computer Science Department. This reflects the dominant academic background of the respondents. Meanwhile, most students (84.4%) attended public institutions, while 15.6% were from private institutions, indicating that the results predominantly reflect perspectives from public school settings.

Downloaded from http://www.emerald.com/jices/article-pdf/doi/10.1108/JICES-10-2025-0279/11507623/jices-10-2025-0279en.pdf by guest on 10

Table 1. Respondents' demographic characteristics ($n = 450$)

Variable	Category	Frequency	%
Age	< 18 years	106	23.6
	18–22 years	295	65.6
	23–27 years	48	10.7
	28–32 years	1	0.2
Gender	Male	177	39.3
	Female	273	60.7
Level of study	Undergraduate (diploma/ND/NCE)	96	21.3
	Undergraduate (bachelor's degree)	351	78.0
	Postgraduate (master's)	2	0.4
	Postgraduate (PhD)	1	0.2
Faculty/Department	Computer	39	8.7
	Mass communication	411	91.3
Type of institution	Public	380	84.4
	Private	70	15.6

Table 2. Student awareness and exposure to surveillance technologies ($n = 450$)

Item	Category	Frequency	%
Awareness of surveillance technologies in your institution	Yes	402	89.3
	No	15	3.3
	Not sure	33	7.3
Frequency of noticing surveillance technologies in daily academic life	Very frequently	193	42.9
	Occasionally	152	33.8
	Rarely	93	20.7
	Never	12	2.7

Students' awareness of surveillance technologies in their institution

This section explores students' levels of awareness and perceived exposure to various surveillance technologies within their academic environment.

Table 2 shows that a substantial majority of students (89.3%) reported being aware of surveillance technologies within their institution, while only a small fraction indicated they were not aware (3.3%) or unsure (7.3%). Regarding exposure, 42.9% of students stated they noticed surveillance technologies very frequently in their daily academic lives, and 33.8% reported noticing them occasionally.

Meanwhile, 20.7% noticed them rarely, and just 2.7% indicated they never noticed them. These findings suggest a high level of both awareness and routine exposure to surveillance technologies among students.

Perceptions of surveillance technologies and their impact on personal privacy

This section explores how students perceive the impact of surveillance technologies on their personal privacy, behavioural responses and confidence in the proper use of surveillance data.

Table 3 presents students' perceptions regarding how surveillance technologies impact their personal privacy. Over half of the respondents (54.9%) felt that their right to privacy was moderately respected, while 32.2% believed it was respected very much. However,

Downloaded from http://www.emerald.com/jices/article-pdf/doi/10.1108/JICES-10-2025-0279/11507623/jices-10-2025-0279en.pdf by guest on 10

Table 3. Students' perceptions of surveillance technologies and their effects on personal privacy

Question	Response option	Frequency	%
To what extent do you feel your right to privacy is respected?	Very much	145	32.2
	Moderately	247	54.9
	Slightly	44	9.8
	Not at all	14	3.1
Have you ever altered your behaviour because you felt you were watched?	Yes	109	24.2
	No	265	58.9
	Not sure	76	16.9
Confidence that data from surveillance will not be misused	Very confident	187	41.6
	Somewhat confident	105	23.3
	Not confident	3	0.7
	Do not know	155	34.4

9.8% felt only slightly respected, and a small portion (3.1%) reported that their privacy was not respected at all. This suggests that while most students feel their privacy is reasonably protected, a notable minority express concerns about inadequate privacy protections.

Also from Table 3, in terms of behavioural impact, 24.2% of students admitted to changing their behaviour due to the feeling of being watched, indicating a psychological or behavioural response to surveillance presence. However, a majority (58.9%) reported no such change, and 16.9% were unsure. Regarding data trust, 41.6% of students expressed strong confidence that surveillance data would not be misused, while 23.3% were somewhat confident. However, 34.4% stated they did not know, and 0.7% had no confidence at all, highlighting uncertainty and potential mistrust among a significant portion of the student body regarding data security and responsible usage.

Influence of demographic characteristics on students' perceptions of surveillance technology and privacy

This section explores how students' demographic characteristics influence their perceptions of surveillance technology and its impact on privacy, behaviour and data security.

Table 4 indicates that demographic characteristics significantly influenced students' perceptions of surveillance technology. Specifically, there were statistically significant effects of age, $F(3, 446) = 4.215$, $p = 0.006$; gender, $F(1, 448) = 5.032$, $p = 0.025$; level of study, $F(3, 446) = 3.761$, $p = 0.012$; and type of institution, $F(1, 448) = 6.109$, $p = 0.014$. However, faculty/department did not show a significant effect, $F(1, 448) = 0.713$, $p = 0.399$. These findings suggest that factors such as age, gender, educational level and institutional

Table 4. Influence of demographic characteristics on students' perceptions of surveillance technology

Demographic variable	*df* (between)	*df* (within)	F-statistic	*p*-value
Age	3	446	4.215	0.006*
Gender	1	448	5.032	0.025*
Level of study	3	446	3.761	0.012*
Faculty/Department	1	448	0.713	0.399
Type of institution	1	448	6.109	0.014*

Note(s): The dependent variable is Perception, computed as the mean of items; *Significant at $p < 0.05$

Downloaded from http://www.emerald.com/jices/article-pdf/doi/10.1108/JICES-10-2025-0279/11507623/jices-10-2025-0279en.pdf by guest on 10

type are associated with differing perceptions of how surveillance technology impacts student privacy.

Table 5 presents the results of chi-square tests assessing the influence of demographic factors on students' perceptions of surveillance technology's impact on privacy. Regarding the right to privacy, significant associations were found for age, $\chi^2(9) = 18.76$, $p = 0.028$; gender, $\chi^2(3) = 9.43$, $p = 0.024$; and institution type, $\chi^2(3) = 13.68$, $p = 0.003$. No significant relationships were observed for level of study or faculty.

Furthermore, for behaviour alteration, Table 5 indicates that only gender, $\chi^2(2) = 6.21$, $p = 0.045$ and institution type, $\chi^2(2) = 7.93$, $p = 0.019$, showed significant effects. Age, level of study and faculty were not significantly associated with changes in behaviour due to surveillance. Regarding confidence in data misuse, significant effects were found for age, $\chi^2(9) = 17.29$, $p = 0.044$ and institution type, $\chi^2(3) = 11.03$, $p = 0.012$, while gender, level of study and faculty did not show significant associations.

Overall, the findings suggest that age, gender and institution type significantly influence students' perceptions of surveillance impact. Thus, the hypothesis (*H3*) is accepted, confirming that students view surveillance technologies as affecting their personal privacy.

Table 6 reveals students' perceptions regarding the types of surveillance technologies used in their institutions. Most respondents (54.3%) indicated that CCTV cameras only were in use, suggesting that visual monitoring is the most recognisable or visible form of surveillance. Some students also perceived combinations of surveillance tools, such as CCTV with biometric attendance systems (8.2%), CCTV with internet activity monitoring (7.0%) and CCTV with learning analytics tools (4.4%). These findings imply that while CCTV remains dominant, a subset of institutions may be using additional layers of digital surveillance to monitor academic activities and student presence.

Furthermore, Table 6 shows a minority recognising more advanced systems. For instance, 3.5% believed that their institutions use a combination of CCTV, biometric systems, internet monitoring and learning analytics tools, while 2.3% noted even more comprehensive surveillance, including facial recognition and location tracking. Technologies used alone,

Table 5. Influence of demographic factors on students' perception of surveillance technology's impact on privacy

Perceived impact on privacy	Demographic factors	Chi-square	df	*p*-value
Right to privacy	Age	18.764	9	*0.028*
	Gender	9.432	3	*0.024*
	Level of study	7.892	9	0.544
	Faculty	3.441	3	0.329
	Institution type	13.682	3	*0.003*
Behaviour alteration	Age	8.334	6	0.214
	Gender	6.213	2	*0.045*
	Level of study	5.872	6	0.438
	Faculty	2.067	2	0.356
	Institution type	7.928	2	*0.019*
Data misuse confidence	Age	17.291	9	*0.044*
	Gender	2.033	3	0.565
	Level of study	9.124	9	0.428
	Faculty	1.774	3	0.621
	Institution type	11.034	3	*0.012*

Note(s): Significant at $p < 0.05$

Downloaded from http://www.emerald.com/jices/article-pdf/doi/10.1108/JICES-10-2025-0279/11507623/jices-10-2025-0279en.pdf by guest on 10

Table 6. Frequency of surveillance technology use in institutions

Technology combination		Frequency	%
(1)	CCTV cameras only	185	54.3
(2)	CCTV cameras + biometric attendance systems	28	8.2
(3)	CCTV cameras + internet activity monitoring	24	7.0
(4)	CCTV cameras + learning analytics tools	15	4.4
(5)	Biometric attendance systems only	10	2.9
(6)	Internet activity monitoring only	6	1.8
(7)	Learning analytics tools only	6	1.8
(8)	CCTV cameras + biometric attendance systems + internet activity monitoring + learning analytics tools	12	3.5
(9)	CCTV cameras + biometric attendance systems + internet activity monitoring + facial recognition + learning analytics + location tracking	8	2.3
(10)	Location tracking only	1	0.3
(11)	None of the above	12	3.5
(12)	Other combinations (e.g. CCTV + facial recognition, CCTV + location tracking, etc.)	33	9.7

such as biometric systems (2.9%), internet activity monitoring (1.8%), learning analytics (1.8%) or location tracking (0.3%), were less frequently perceived. Additionally, 3.5% of respondents stated that none of the listed technologies were present in their institutions, and 9.7% identified other combinations, such as CCTV with facial recognition or location tracking. This suggests that while traditional surveillance is widely acknowledged, awareness of more sophisticated and integrated systems is relatively limited.

The findings support the first hypothesis (*H1*), indicating significant student awareness of surveillance technologies. As shown in Table 2, 89.3% of students acknowledged awareness, and most reported frequent or occasional exposure. This confirms the visibility and recognition of surveillance systems across institutions.

Relationship between awareness of surveillance technologies and frequency of student exposure

In this section, the relationship between students' awareness of surveillance technologies and how frequently they notice them in their academic environment was examined using a chi-square test of independence.

The results in Table 7 indicate a statistically significant relationship between students' awareness and their reported frequency of noticing surveillance technologies on campus. The Pearson Chi-Square value of 47.80 with 6 degrees of freedom and a *p*-value less than

Table 7. Association between student awareness and frequency of observing surveillance technologies on campus

Test statistic	χ^2	df	*p*
Pearson Chi-Square	47.80	6	< 0.001
Likelihood ratio	35.72	6	< 0.001
Linear-by-linear association	31.57	1	< 0.001

Downloaded from http://www.emerald.com/jices/article-pdf/doi/10.1108/JICES-10-2025-0279/11507623/jices-10-2025-0279en.pdf by guest on 10

0.001 confirms that the association is highly significant. Similarly, the Likelihood Ratio and the Linear-by-Linear Association tests also yield p-values below 0.001, reinforcing this conclusion.

Hence, From Table 7 since all *p*-values are well below the conventional threshold of 0.05, we reject the null hypothesis and accept (*H2*), confirming that students who are more aware of surveillance technologies are significantly more likely to report frequent observations of these technologies in their academic environment.

Influence of students' attitudes on their comfort with surveillance (trust, consent, transparency)

This section explores whether students' attitudes, specifically trust, transparency and consent, influence their comfort with surveillance. Understanding these relationships helps identify key psychological factors shaping students' acceptance of monitoring practices.

Table 8 showed significant differences in comfort levels based on trust ($\chi^2(4) = 223.86$, $p < 0.001$), perceived transparency ($\chi^2(4) = 206.01$, $p < 0.001$) and belief in consent ($\chi^2(4) = 174.11$, $p < 0.001$). In each case, higher levels of trust, transparency and consent were found to positively influence students' comfort with surveillance. These findings indicate that students' attitudes significantly influence how comfortable they feel being monitored. Therefore, the null hypothesis (*H4*) is rejected.

Relationship between institutional trust and confidence in data protection

This section examines whether students' trust in their institution's handling of surveillance data is significantly related to their confidence in data protection.

Table 9 presents students' perceptions of surveillance technologies across several dimensions. Overall, the total mean score of 3.18 indicates a generally positive perception of surveillance, falling within the "Good" range (see, Table 9 above). The highest-rated statements include the belief that surveillance helps keep the campus safe (Mean = 4.09) and trust in the institution's responsible data handling (Mean = 3.83), both reflecting strong institutional confidence and acceptance of surveillance as a safety tool.

On the other hand, from Table 9, students expressed moderate concerns regarding privacy invasion (Mean = 2.68), discomfort with being monitored (Mean = 2.65) and surveillance's influence on academic performance (Mean = 2.60), showing that while surveillance is generally accepted, a notable proportion of students remain cautious about its personal impacts. Interestingly, responses about transparency (Mean = 3.40) and consent (Mean = 3.06) highlight the demand for more clarity and autonomy in surveillance practices. These findings suggest a balanced view: students recognise the utility of surveillance but still desire safeguards for personal rights and data protection.

Table 8. Test statistics examining the influence of trust, transparency and consent on student comfort with surveillance

Variable	Kruskal–Wallis *H*	df	*p*-value
Trust in institution to handle surveillance data responsibly	223.858	4	0.000
Transparency about how surveillance is used	206.008	4	0.000
Consent before being subjected to surveillance	174.110	4	0.000

Note(s): All effects significant at $p < 0.001$

Downloaded from http://www.emerald.com/jices/article-pdf/doi/10.1108/JICES-10-2025-0279/11507623/jices-10-2025-0279en.pdf by guest on 10

Table 9. Students' perceptions of surveillance technology ($n = 450$)

Statement	SD (%)	D (%)	N (%)	A (%)	SA (%)	Mean	Remarks
Surveillance helps keep the campus safe	31 (6.9)	8 (1.8)	34 (7.6)	194 (43.1)	183 (40.7)	4.09	Very good
I feel uncomfortable being monitored by surveillance technologies	75 (16.7)	142 (31.6)	129 (28.7)	72 (16.0)	32 (7.1)	2.65	Good
Surveillance invades my personal privacy	94 (20.9)	120 (26.7)	111 (24.7)	85 (18.9)	40 (8.9)	2.68	Good
The benefits of surveillance outweigh its risks	74 (16.4)	94 (20.9)	75 (16.7)	124 (27.6)	83 (18.4)	3.11	Good
My academic performance is influenced by being monitored	113 (25.1)	133 (29.6)	76 (16.9)	78 (17.3)	50 (11.1)	2.60	Good
I trust my institution to handle surveillance data responsibly	39 (8.7)	19 (4.2)	55 (12.2)	201 (44.7)	136 (30.2)	3.83	Very good
There is enough transparency about how surveillance is used	40 (8.9)	55 (12.2)	115 (25.6)	164 (36.4)	76 (16.9)	3.40	Good
I should be asked for consent before being subjected to surveillance	66 (14.7)	92 (20.4)	110 (24.4)	112 (24.9)	70 (15.6)	3.06	Good
Total mean score						*3.18*	*Good*

Downloaded from http://www.emerald.com/jices/article-pdf/doi/10.1108/JICES-10-2025-0279/11507623/jices-10-2025-0279en.pdf by guest on 10

Table 10. Relationship between trust and confidence in surveillance data use

Variables	Trust	Confidence
Trust	–	0.144**
Confidence	0.144**	–

Note(s): ρ = Spearman's rho; $p < 0.01$

Thus, to assess whether students' perception of institutional data responsibility relates significantly to their confidence that surveillance data will not be misused, Spearman's rank-order correlation was conducted.

Table 10 revealed a statistically significant positive correlation between trust in institutional data handling and confidence in data protection, $\rho\ (450) = 0.144$, $p = 0.002$. Although the strength of the association is weak, the significance suggests that higher levels of trust are associated with increased confidence that data collected through surveillance will not be misused. Therefore, the null hypothesis (*H5*) is rejected, supporting the claim that students' trust in institutional data practices significantly influences their confidence in data protection.

Students' beliefs on policy regulation of surveillance and the role of student input

Based on the results presented in Table 11, there is strong evidence to support *H5*, which states that students significantly support policy regulation of surveillance involving student input. A substantial majority (68.9%) of the respondents agreed that surveillance in educational institutions should be governed by policies that include student participation. Given this clear majority and the relatively small proportion of dissenting views (12.0%), the hypothesis is not rejected, confirming that students favour inclusive policy frameworks for surveillance practices.

In follow-up responses, students generally supported surveillance for safety but emphasised the need for transparency, privacy protection and involvement in policymaking. Many called for clear guidelines on monitoring scope, data usage and access. Concerns were raised about surveillance in sensitive areas, and the importance of informed consent and ethical data use was stressed.

Technical improvements were also suggested, including upgraded cameras, solar power, better connectivity and real-time or AI-based monitoring. Students recommended regular footage reviews and enhanced maintenance.

While most had no additional comments, some highlighted the need to balance security with privacy through clear communication, responsible monitoring and student participation

Table 11. Students' opinions on the need for policy regulation of surveillance with student input

Response	Frequency	%
Yes	310	68.9
No	54	12.0
Not sure	86	19.1
Total	450	100.0

Downloaded from http://www.emerald.com/jices/article-pdf/doi/10.1108/JICES-10-2025-0279/11507623/jices-10-2025-0279en.pdf by guest on 10

in shaping surveillance policies. Overall, students want effective surveillance that respects their rights and builds trust.

Table 12 above provides a comprehensive guide for the interpretation of mean scores which was obtained from the perception statements measured using five-point Likert scale. Its implies that numerical averages from the respondents' ratings can be interpreted into a clear qualitative meaning, making the findings very easy to understand and review.

For instance, a mean score between 2.61 and 3.40 implies that respondents' perception is good, while a mean between 4.21 and 5.00 indicates an excellent perception. This interpretation framework can assist the researcher group respondents' attitudes or perceptions into a very meaningful categories, confirming a consistent in data analysis and reporting. By and large, the table serves as a decision guide for describing the result from the survey, letting the researcher to move from raw numerical data to a more interpretable conclusions about respondents' perceptions.

Discussion

This research carefully explored students' perceptions of surveillance technologies in an academic environment, particularly how it impacts their sense of privacy and autonomy. In Table 2 for instance, it reveals expressive demographic variation in student perceptions of surveillance technology: age, gender, level of study and institution type matter, while faculty does not. These findings reverberate a wider opinion from literature on privacy and surveillance attitudes are socially patterned and context-dependent (Acquisti *et al.*, 2015; Birnhack and Perry-Hazan, 2020). The general implication for policymakers and practitioners is that surveillance governance in education should be evidence-based, transparent and differentiated, coupling technological deployment with student engagement, tailored communication and robust privacy protections. For the researchers, results from ANOVA provide a valuable starting point, but deeper multivariate and qualitative work is necessary to explain further why these demographic differences arise and how they translate into behaviour and institutional outcomes.

Using UTAUT as an interpretive lens, the discussion shows that while demographic moderators remain robust, the model must be critically extended to account for privacy, power, governance and ethical legitimacy, revealing technology acceptance in surveillance contexts as contingent, coerced and institutionally structured rather than purely voluntary or efficiency driven.

Concerning the right to privacy, the significant influence of age ($\chi^2(9) = 18.76$, $p = 0.028$) aligns with previous studies, which suggests that younger digital natives often perceive surveillance differently in relation to older students, who may be more cautious about their digital footprints (Deogracias, 2015). Younger students tend to normalise surveillance as part of their daily digital experience, while older students, on the other hand, may be more sensitive to potential intrusions into their private autonomy. Likewise, the role of gender

Table 12. Verbal interpretation guide for five-point Likert scale on perception statements

Mean score	Perception
1.0–1.80	Very poor
1.81–2.60	Poor
2.61–3.40	Good
3.41–4.20	Very good
4.21–5.00	Excellent

Downloaded from http://www.emerald.com/jices/article-pdf/doi/10.1108/JICES-10-2025-0279/11507623/jices-10-2025-0279en.pdf by guest on 10

($\chi^2(3) = 9.43$, $p = 0.024$) is consistent with findings from extant literature by Masiero and Bailur (2021), who observed that women often express aggravated concerns over privacy, especially in relation to where surveillance interconnects with issues of safety and vulnerability. The influence of institution type ($\chi^2(3) = 13.68$, $p = 0.003$) clearly suggests that organisational philosophy and governance structures, whether in public or private institutions, affect how surveillance is justified and perceived. Research by Yazdanmehr, *et al.* (2020) confirms that institutional norms often shape students' acceptance or resistance to surveillance measures.

The findings show that students' acceptance of surveillance technologies is not uniform but is significantly moderated by age, gender and institutional context, with privacy perceptions shaped less by technological efficiency and more by digital socialisation, gendered risk awareness and the strength of organisational governance and safeguards.

In relation to behavioural alteration, only gender ($\chi^2(2) = 6.21$, $p = 0.045$) and institution type ($\chi^2(2) = 7.93$, $p = 0.019$) were significant. This indicates that surveillance technologies may lead to self-regulation of behaviour, but such effects are not uniformly distributed across demographics. Women, for instance, may be more likely to adapt their online or offline conduct under surveillance, reflecting broader patterns of gendered socialisation and risk perception (Stoycheff, 2020). Institution type further reinforces the idea that surveillance policies and enforcement vary across educational environments, leading to differential impacts on students' behaviour (Andrejevic, 2019).

Regarding confidence in data misuse, both age ($\chi^2(9) = 17.29$, $p = 0.044$) and institution type ($\chi^2(3) = 11.03$, $p = 0.012$) showed significant associations. This suggests that older students may be more aware of the risks associated with data breaches and unauthorised use of personal information. Such concerns echo global anxieties around data governance and institutional accountability in the digital age (Zuboff, 2019). The significant role of institution type again highlights the importance of trust in institutional data handling practices, as students in private institutions may perceive stronger safeguards compared to those in public institutions, or vice versa, depending on governance frameworks (Livingstone *et al.*, 2019).

Anchored in UTAUT, these findings underscore that students' behavioural self-regulation and privacy concerns are shaped by moderated pathways of social influence, facilitating conditions and perceived risk. The unequal distribution of effects across demographic and institutional categories challenges universalist assumptions of surveillance acceptance and calls for context-sensitive policy and ethical governance frameworks in educational institutions.

The results indicate that most students (89.3%) are aware of surveillance technologies in their institutions, with many encountering them frequently or occasionally. This aligns with studies showing that surveillance has become a normalised part of daily academic life (Lyon, 2018). The widespread recognition of CCTV cameras (54.3%) as the dominant form of monitoring reflects global reliance on visual surveillance (Hope, 2019). However, fewer students recognised less visible tools such as biometrics, internet monitoring or learning analytics, raising concerns about transparency. Scholars caution that such technologies are often more intrusive, as they extend beyond physical observation to data profiling (Andrejevic, 2019).

A smaller group of students noted awareness of integrated or advanced systems combining multiple surveillance tools, reflecting what Zuboff (2019) terms "surveillance capitalism," where institutions maximise oversight through data convergence. Though only a minority reported awareness of these systems, their recognition points to growing unease about the expansion of digital surveillance in education.

Downloaded from http://www.emerald.com/jices/article-pdf/doi/10.1108/JICES-10-2025-0279/11507623/jices-10-2025-0279en.pdf by guest on 10

Critically, these findings raise ethical and pedagogical concerns. Drawing on Foucault's (1977; Foucault, 2019) panopticons, constant monitoring can encourage self-regulation but also risks eroding trust and autonomy. Research further shows that students often view surveillance as intrusive, undermining academic freedom and belonging (Selwyn and Cumbo, 2024). The gap between visible and less perceptible monitoring highlights issues of informed consent and transparency. Effective governance, as Ball (2021) argues, requires open communication about what is monitored, why it is necessary and how data are used.

The results indicate a significant association between students' awareness of surveillance technologies and their frequency of observing them on campus ($\chi^2 = 47.80$, df = 6, $p < 0.001$), suggesting that heightened awareness increases the likelihood of noticing surveillance devices. This aligns with prior scholarship that links awareness to intensified perceptions of surveillance and the panoptic effect, whereby individuals internalise the presence of monitoring and adjust their behaviour accordingly (Foucault, 2019; Lyon, 2018; Monahan, 2017).

Students' perceptions of privacy reveal a mixed landscape: while most respondents (54.9%) felt their privacy was moderately respected, a notable minority expressed concern over inadequate protection, and nearly a quarter (24.2%) reported behavioural changes due to being watched. These findings reflect documented "chilling effects" of surveillance (Penney, 2017) and reinforce the role of monitoring as both a protective and disciplinary mechanism (Selwyn, 2021; Zuboff, 2019).

Confidence in data handling also varied, with 41.6% expressing strong trust, but a significant proportion remaining uncertain (34.4%) or sceptical (0.7%). Such ambivalence resonates with critiques of opaque governance practices in surveillance systems, underscoring the need for institutional transparency and accountability (Andrejevic, 2019; Ball, 2021).

Overall, the study highlights three implications:

- awareness shapes both perceptions and experiences of surveillance;
- privacy is perceived inconsistently, with potential psychological and behavioural consequences; and
- trust in data governance remains fragile.

These findings situate surveillance in education as both a security measure and a form of social control, revealing tensions between institutional objectives and students' rights.

The results presented in Table 10 demonstrate a statistically significant positive relationship between trust in institutional data handling and confidence in data protection ($\rho = 0.144$, $p < 0.01$). Although the strength of this correlation is weak, the significance suggests that students' trust in how institutions manage surveillance data is closely tied to their confidence that such data will not be misused. This aligns with broader research indicating that trust functions as a precursor to perceptions of fairness and legitimacy in surveillance practices (Smith *et al.*, 2020). Even when associations are weak, significance can indicate that trust acts as a foundational variable shaping attitudes towards digital surveillance (Lyon, 2018).

While the statistically significant association confirms a meaningful link between trust and confidence in data protection, the weak correlation and potential biases suggest that this relationship should be interpreted as indicative rather than determinative. The finding supports the argument that trust matters, but it also highlights the need for multi-dimensional models that incorporate structural safeguards, legal frameworks and students' critical awareness of surveillance technologies.

Downloaded from http://www.emerald.com/jices/article-pdf/doi/10.1108/JICES-10-2025-0279/11507623/jices-10-2025-0279en.pdf by guest on 10

One critical point, however, is that the weak strength of association may reflect latent scepticism among students, revealing a gap between institutional assurances and students' lived experiences with data practices. Prior studies have shown that transparency deficits in surveillance erode confidence, particularly when students perceive an imbalance of power or lack of accountability in institutional data use (Livingstone and Third, 2017). Thus, while the positive correlation indicates progress, the relatively low coefficient underscores the need for greater transparency, participatory communication and accountability frameworks.

The findings from Table 11 strengthen this interpretation by revealing that 68.9% of students favour policy regulation of surveillance with active student input. This strong endorsement reflects growing demands for inclusivity and participatory governance in digital monitoring environments. Similar studies in higher education show that students prefer surveillance systems that are co-designed with stakeholders and emphasise ethical safeguards, rather than unilateral impositions by administrators (Taylor and Rooney, 2016). Such findings echo calls within surveillance studies to move away from top-down control towards deliberative governance structures that incorporate the voices of those being monitored (Andrejevic, 2019).

The qualitative responses further reveal a nuanced perspective. While students acknowledge the utility of surveillance for safety, they insist on clear boundaries regarding scope, usage and access. Their concerns about surveillance in sensitive spaces, emphasis on informed consent and calls for ethical data governance are consistent with emerging debates on privacy in educational contexts (Selwyn, 2019). Importantly, the suggestion for technical improvements, such as AI-based monitoring or solar-powered systems, signals not just acceptance of surveillance, but a desire for its modernisation, provided it is accompanied by strong ethical and regulatory safeguards.

Taken together, the findings suggest that trust, confidence and participation are interdependent factors shaping students' acceptance of surveillance. The weak but significant correlation in Table 10 underscores the fragility of confidence in surveillance regimes, while the strong majority in Table 11 reflects students' demand for participatory and transparent governance frameworks. This aligns with the critical discourse that surveillance, when divorced from ethical practice, risks normalising control and exacerbating feelings of disempowerment (Zuboff, 2019). Yet, when reframed through inclusive policymaking, surveillance can be repositioned as a tool that enhances not only safety but also mutual trust and institutional legitimacy.

Conclusion

This study examined students' perceptions of surveillance technologies within academic institutions, highlighting how demographic variables such as age, gender, level of study and institution type shape attitudes towards privacy, behaviour and trust in data governance. The findings reveal that surveillance is widely recognised and normalised in educational spaces, with CCTV as the most visible form of monitoring, though less visible systems such as biometrics and online tracking remain under-acknowledged. Importantly, perceptions of surveillance are socially patterned: younger students tend to normalise monitoring, while older students express heightened privacy concerns; women demonstrate greater sensitivity to behavioural changes under surveillance; and institutional type significantly influences levels of trust and acceptance.

Although many students acknowledge the safety benefits of surveillance, concerns persist over transparency, consent and potential misuse of data. The weak but significant correlation between trust in institutional data handling and confidence in data protection

Downloaded from http://www.emerald.com/jices/article-pdf/doi/10.1108/JICES-10-2025-0279/11507623/jices-10-2025-0279en.pdf by guest on 10

reflects fragile confidence in governance practices. Moreover, the majority preference for regulatory frameworks with active student participation underscores a growing demand for inclusivity and accountability in surveillance governance. Overall, surveillance in education emerges as a double-edged phenomenon: while it enhances safety and order, it simultaneously raises ethical, psychological and social challenges that call for deliberate governance strategies.

Limitations of the study

The study is limited by disciplinary bias due to the predominance of communication students, restricted cultural and institutional diversity, reliance on self-reported data, which is susceptible to social desirability bias and a cross-sectional design that precludes analysis of changes in surveillance perceptions over time.

Recommendations

(1) Institutions should adopt clear and accessible communication strategies about the scope, purpose and use of surveillance technologies. Regular disclosure of monitoring practices can bridge the trust gap and reduce scepticism among students.

(2) Governance frameworks should involve active student participation in the design, implementation and review of surveillance policies. Co-creation of policies fosters legitimacy, inclusivity and stronger acceptance among stakeholders.

(3) Given the influence of demographic factors, institutions should tailor communication and policy enforcement to different student groups, ensuring that diverse concerns such as age-related or gender-based differences are addressed fairly.

(4) Surveillance must be accompanied by robust privacy protections, including data minimisation, anonymisation and strict access controls. Institutions should provide avenues for grievance redress when students feel their rights have been compromised.

(5) Students should be educated about both visible and less visible surveillance tools, enabling informed consent and awareness of potential risks. This can be integrated into digital literacy programmes.

(6) Institutions should conduct regular audits and impact assessments of surveillance technologies to evaluate their effectiveness, ethical implications and alignment with institutional values.

(7) Governments and educational authorities should establish clear regulations guiding the deployment and management of surveillance technologies in educational settings, with emphasis on accountability, inclusivity and data protection.

Disclosure of AI use

The author used an artificial intelligence–assisted writing tool exclusively for grammatical correction and language refinement. No AI system was used to generate research ideas, data, analysis or conclusions. The author takes full responsibility for the accuracy and integrity of the work.

Funding

This research was conducted without external financial support. All costs associated with data collection, analysis, and reporting were covered by the researcher.

Downloaded from http://www.emerald.com/jices/article-pdf/doi/10.1108/JICES-10-2025-0279/11507623/jices-10-2025-0279en.pdf by guest on 10

References

Acquisti, A., Brandimarte, L. and Loewenstein, G. (2015), "Privacy and human behavior in the age of information", *Science*, Vol. 347 No. 6221, pp. 509-514.

Andrejevic, M. (2019), "Automating surveillance", *Surveillance and Society*, Vol. 17 Nos 1-2, pp. 7-13, doi: 10.24908/ss.v17i1/2.12930.

Ball, K. (2021), "Electronic monitoring and surveillance in the workplace: literature review and policy recommendations", available at: https://research-repository.st-andrews.ac.uk/handle/10023/32743

Bayaga, A. and Du Plessis, A. (2024), "Ramifications of the unified theory of acceptance and use of technology (UTAUT) among developing countries' higher education staffs", *Education and Information Technologies*, Vol. 29 No. 8, pp. 9689-9714.

Birnhack, M. and Perry-Hazan, L. (2020), "School surveillance in context: high school students' perspectives on CCTV, privacy, and security", *Youth and Society*, Vol. 52 No. 7, pp. 1312-1330.

Deogracias, A. (2015), *Danah Boyd: It's Complicated: The Social Lives of Networked Teens*, Yale University Press, New Haven, CT, p. 296. ISBN 973-0-300-16631-6.

Fernando, F., Lizandro, L., Thayná, G.R. and Gabriela, C.F. (2025), "The institutional design of data governance in Brazil: entropy, restrictiveness and institutional grammar", *Policy Design and Practice*, Vol. 8 No. 1, pp. 64-88.

Fontes, C., Hohma, E., Corrigan, C.C. and Lütge, C. (2022), "AI-powered public surveillance systems: why we (might) need them and how we want them", *Technology in Society*, Vol. 71, p. 102137, doi: 10.1016/j.techsoc.2022.102137.

Foucault, M. (2019), "Panopticism (1977)", In *Crime and Media*, Routledge, pp. 493-505, available at: www.taylorfrancis.com/chapters/edit/10.4324/9780367809195-43/panopticism-1977-michel-foucault

Hope, A. (2015), "Governmentality and the 'selling' of school surveillance devices", *The Sociological Review*, Vol. 63 No. 4, pp. 840-857.

Ilci, A. (2020), "Protecting privacy: a case study on data collection and surveillance in educational environments", Doctoral dissertation, University of Illinois at Urbana-Champaign.

Khan, A.U., Hussain, U., Rashid, M. and Hameed, R. (2024), "Social norms and legal compliance: understanding the psychological factors influencing adherence to laws in educational settings", *Bulletin of Business and Economics (BBE)*, Vol. 13 No. 3, pp. 326-332.

Lai, X. and Rau, P.-L.P. (2021), "Has facial recognition technology been misused? A public perception model of facial recognition scenarios", *Computers in Human Behavior*, Vol. 124, p. 106894, doi: 10.1016/j.chb.2021.106894.

Lee, L.M., Heilig, C.M. and White, A. (2012), "Ethical justification for conducting public health surveillance without patient consent", *American Journal of Public Health*, Vol. 102 No. 1, pp. 38-44.

Livingstone, S. and Third, A. (2017), "Children and young people's rights in the digital age: an emerging agenda", *New Media and Society*, Vol. 19 No. 5, pp. 657-670.

Livingstone, S., Kardefelt-Winther, D., Kanchev, P., Cabello, P., Claro, M., Burton, P. and Phyfer, J. (2019), "Is there a ladder of children's online participation? Findings from three global kids online countries", *Innocenti Research Briefs*, doi: 10.18356/99c54772-en.

Lyon, D. (2018), "The culture of surveillance: watching as a way of life", John Wiley and Sons, available at: www.wiley.com/enus/The±Culture±of±Surveillance%3A±Watching±as±a±Way±of±Life-p-9780745671734

Mantello, P., Ho, M.T., Nguyen, M.H. and Vuong, Q.H. (2023), "Machines that feel behavioural determinants of attitude towards affect recognition technology-upgrading technology acceptance theory with the mindsponge model", *Humanities and Social Sciences Communications*, Vol. 10 No. 1, doi: 10.1057/s41599-023-01837-1.

Downloaded from http://www.emerald.com/jices/article-pdf/doi/10.1108/JICES-10-2025-0279/11507623/jices-10-2025-0279en.pdf by guest on 10

Martin, K. and Shilton, K. (2016), "Why experience matters to privacy: how context-based experience moderates consumer privacy expectations for mobile applications", *Journal of the Association for Information Science and Technology*, Vol. 67 No. 8, pp. 1871-1882.

Masiero, S. and Bailur, S. (2021), "Digital identity for development: the quest for justice and a research agenda", *Information Technology for Development*, Vol. 27 No. 1, pp. 1-12.

Monahan, T. (2017), "Regulating belonging: surveillance, inequality, and the cultural production of abjection", *Journal of Cultural Economy*, Vol. 10 No. 2, pp. 191-206.

Nayyar, A., Nguyen, B.L. and Nguyen, N.G. (2019), "The internet of drone things (IoDT): future envision of smart drones", In First International Conference on Sustainable Technologies for Computational Intelligence: Proceedings of ICTSCI 2019. *Singapore*: *Springer Singapore*, pp. 563-580.

Niemi, H., Pea, R.D. and Lu, Y. (2023), *AI in Learning: designing the Future*, Springer Nature, pp. 344.

Nunn, S. (2001), "Police technology in cities: changes and challenges", *Technology in Society*, Vol. 23 No. 1, pp. 11-27, doi: 10.1016/S0160-791X(00)00033-6.

Odoemelam, C.E. (2015), "Adapting to surveillance and privacy issues in the era of technological and social networking", *International Journal of Social Science and Humanity*, Vol. 5 No. 6, pp. 521-527.

Penney, J. (2017), "Internet surveillance, regulation, and chilling effects online: a comparative case study. Regulation, and chilling effects online: a comparative case study (may 27, 2017)", *Internet Policy Review*, Vol. 6 No. 2.

Reith, R., Buck, C., Eymann, T. and Lis, B. (2020), "Integrating privacy concerns into the unified theory of acceptance and use of technology to explain the adoption of fitness trackers", *International Journal of Innovation and Technology Management*, Vol. 17 No. 07, p. 2050049.

Saputra, E. and Handayani, F. (2024), "The impact of digital surveillance on privacy rights: a legal and ethical analysis", *Proceedings of the International Conference on Law and Human Rights*, Vol. 1 No. 2, pp. 8-12, doi: 10.62383/iclehr.v1i2.22.

Sarifudin, R. and Damanik, F.H.S. (2024), "Enhancing transparency and accountability in public administration through information technology utilization", *Gema Wiralodra*, Vol. 15 No. 1, pp. 32-40.

Selwyn, N. and Cumbo, B. (2024), "We've tried to keep the beast on a leash": the domestication of digital classroom surveillance", *Surveillance and Society*, Vol. 22 No. 2, pp. 88-103.

Shao, X.F., Li, Y., Suseno, Y., Li, R.Y.M., Gouliamos, K., Yue, X.G., *et al*. (2021), "How does facial recognition as an urban safety technology affect firm performance? The moderating role of the home country's government subsidies", *Safety Science*, Vol. 143, p. 105434, doi: 10.1016/j.ssci.2021.105434.

Smith, D.R., Duval, A., Pouwels, K.B., Guillemot, D., Fernandes, J., Huynh, B.T., Temime, L. and Opatowski, L. and AP-HP/Universities/Inserm COVID-19 Research Collaboration (2020), "Optimizing COVID-19 surveillance in long-term care facilities: a modelling study", *BMC Medicine*, Vol. 18 No. 1, p. 386.

Stoycheff, E. (2020), "Relatively democratic: how perceived internet interference shapes attitudes about democracy", *The International Journal of Press/Politics*, Vol. 25 No. 3, pp. 390-406, doi: 10.1177/1940161220909741.

Taylor, E. and Rooney, T. (2016), *Surveillance Futures: Social and Ethical Implications of New Technologies for Children and Young People*, Routledge.

Venkatesh, V., Morris, M.G., Davis, G.B. and Davis, F.D. (2003), "User acceptance of information technology: toward a unified view", *MIS Quarterly*, Vol. 27 No. 3, pp. 425-478.

Wheatley, M.C. (2024), "Ethics of surveillance technologies: balancing privacy and security in a digital age", available at: https://premierscience.com/wp-content/uploads/2024/11/pjds-24-359.pdf

Downloaded from http://www.emerald.com/jices/article-pdf/doi/10.1108/JICES-10-2025-0279/11507623/jices-10-2025-0279en.pdf by guest on 10

Yazdanmehr, A., Wang, J. and Yang, Z. (2020), "Peers matter: the moderating role of social influence on information security policy compliance", *Information Systems Journal*, Vol. 30 No. 5, pp. 791-844.

Zuboff, S. (2019), "Surveillance capitalism and the challenge of collective action", *New Labor Forum*, Vol. 28 No. 1, pp. 10-29.

Corresponding author
Oluwole Olumide Durodolu can be contacted at: woledurodolu@gmail.com

For instructions on how to order reprints of this article, please visit our website:
www.emeraldgrouppublishing.com/licensing/reprints.htm
Or contact us for further details: **permissions@emeraldinsight.com**

Downloaded from http://www.emerald.com/jices/article-pdf/doi/10.1108/JICES-10-2025-0279/11507623/jices-10-2025-0279en.pdf by guest on 10