Issues in Information Systems
Volume 26, Issue 3, pp.445-456, 2025

DOI: https://doi.org/10.48009/3_iis_2025_136

A policy void: An analysis of biometric facial recognition technology governance in K12 public school handbooks

Valerie Mercer, *Middle Georgia State University, valerie.mercer@mga.edu*

Abstract

Despite widespread facial recognition capabilities in modern surveillance systems and growing state-level restrictions, a content analysis of over 250 K-12 student and staff handbooks revealed none addressed facial recognition or biometric data collection policies or usage. With keyword searches across small, medium, large, rural, suburban, and urban school systems, the analysis showed despite overarching use of surveillance cameras on campuses, in auxiliary locations such as stadiums and fields, and on student transportation vehicles, the public school system handbooks reviewed did not address disclosure of any collection of facial recognition or other biometric data possibilities. These major findings, developed via systematic content analysis, indicate a policy vacuum which points to a systemic problem while providing baseline data for policy reform opportunities at the local, state, and federal levels. This systematic policy void represents a critical gap between widespread surveillance technology deployment and institutional transparency, creating potential legal vulnerabilities and compromising informed consent principles for students and their families as well as staff members. This transparency void suggests potential gaps in institutional oversight of biometric data governance practices leading to cybersecurity vulnerabilities and risks. The study's conclusion points to opportunities for K12 student and staff handbooks to provide disclosure regarding biometric tools used for surveillance, administration, and even instructional purposes.

Keywords: facial recognition, biometric, K12, student handbook, personnel handbook

Introduction

In today's K12 landscape in the United States, surveillance enhanced with artificial intelligence represents a new frontier of possible administrative and academic opportunities. With potential to change teaching and learning as well as safety and administrative processes, this burgeoning and constantly evolving technology, is quickly changing student, staff, and even public safety by facial recognition surveillance and related biometric functions in the K12 setting (Prothero, 2023). In an era of school shootings and increased violence in the school setting, administrators have turned to surveillance tools to monitor school activity in the name of safety (Akgun and Greenhow, 2021). As cameras have become more advanced, the camera systems are now able to recognize faces, store faces, retrieve facial data, and compare facial data (Birnhack and Perry-Hazan, 2020). All these activities are done without the knowledge or consent of the person whose image is captured (Akgun and Greenhow, 2021). With this new way of surveilling school system properties, there are questions surrounding the use of advanced surveillance tools and the related data these tools collect (Birnhack and Perry-Hazan, 2020). With the ability to collect, store, compare, and even share facial recognition data of students, staff, visitors, and the public, the questions arise of disclosure of this technology. Major manufacturers of surveillance cameras are selling their wares with the option to turn on facial recognition and facial database collection (Cisco Meraki, 2025; Avigilon, 2025). Despite the mass purchases of this equipment, school systems may not be informing their personnel, students, and the students' families of this possible usage. Laws and regulations which cover the usage of facial recognition

surveillance technology usage for K12 schools are rare (Fedders, 2019; Prothero, 2023). Given the recent passage of the first state law which forbids student facial recognition technology use in public schools in the State of New York, there is an urgency to review how K12 schools are disclosing the use of facial recognition technology and related biometric data to students, their families, staff, and the public.

Literature Review

Since the invention of the mass produced camera in the 1890s, the privacy of the United States citizen has been questioned as more and more parts of society have come under surveillance (Burrows, 2013). Sociologist David Lyon established surveillance as "focused, systematic and routine attention to personal details for purposes of influence, management, protection, or direction (Lyon, 2007, p. 14)." Surveillance of schools using camera systems, in light of increased violence in the K12 setting over the last thirty years, has become commonplace (Fedders, 2019). Surveillance cameras are used in parking lots, classrooms, entrances, common settings such as cafeterias, hallways, libraries, gymnasiums, and auxiliary locations such as playgrounds, stadiums, driveways, and school buses (Addington, 2024) Surveillance cameras at all levels -- elementary, middle, and high -- have become so commonplace parents and the community expect to see cameras in K12 schools (Prothero, 2023). The advancement of surveillance to include facial recognition and facial matching brings about a new element of possible privacy violation as biometric data of personnel and students, their "faceprints" may be collected and possibly used for purposes other than the intended use of safety measures for schools (Berson, et al., 2025, p. 2).

Modern Day Surveillance in Schools

Modern surveillance systems are easy to deploy, affordable, and these tools have more features than ever before (Nair, 2024). Facial recognition technology has been in use for surveillance deployment since the early 2000s with the most notable first mass event for surveillance being the 2001 Super Bowl (Prothero, 2023). Today, major venues such as retail areas, concert venues, and even metropolitan sidewalks are filled with a 3.2-billion-dollar network of unobtrusive 24/7 instruments which collect footage and facial recognition data (Galligan et al., 2020). Most manufacturers such as Cisco and Avigilon, major surveillance providers in the K12 landscape, are offering facial recognition, pattern monitoring, and biometric collection regardless of the subject's consent or notice of disclosure of this technology (Selinger & Hartzog, 2020; Cisco, 2024, Avigilon, n. d.). These plug-and-play devices enable schools to install, collect, store, and analyze biometric data from students, staff, and visitors as never before (Selinger & Hartzog, 2020). These latest surveillance methods combine facial recognition technology and high-quality video collection with real-time analysis to make more information available about camera subjects than ever before, and then that data is stored. K12 administrators and even law enforcement can have access to the data, and it can be commoditized to be sold or repurposed based on fine print of sales contracts (Keonig, 2020). With cloud-based technology, the video can be analyzed, distributed, and shared to record amounts of receivers and personnel including administrators, law enforcement, and classroom educators. Verkada, a major provider in the K12 market, offers gender appearance tracking and "person of interest" tracking based on a previously uploaded picture to a database owned and stored by Verkada. These affordable cameras are measuring up to 68 datapoints on the face to be as accurate as possible (Lyu, et al., 2024). Object/face tracking is defined by Verkada as the ability to match a face previously seen by the camera with a present face, and the software also claims to be able to track vehicles by storing vehicles in a database as well (Verkada, 2025). With a proliferation of surveillance cameras at affordable prices, school systems have covered their campuses with cameras, and campuses have more monitoring equipment than ever before (Galligan, et al., 2020).

With the passage of Covid-19 relief legislation, schools were able to afford more surveillance camera equipment than ever before as some schools used their funds for safety and other systems used their funds to bring in "instructional surveillance" cameras into the classrooms (Chanenson, et al., 2023). Not only are sophisticated cameras in common areas, but some school systems have chosen to put cameras in every instructional classroom setting such as Bibb County Schools in Macon, Georgia, an urban school system comprised of over 2000 classrooms (Franklin, 2017). With surveillance cameras in public places such as parks, highways, playgrounds, and streets, administrators are looking for surveillance solutions because they have seen and heard of the proliferation of surveillance and its success in solving cold crimes, locating missing people, and preventing criminal activities (Lyu, et al., 2024). Part of the appeal for educational administrators is that surveillance cameras and their abilities to track specific faces offer the solution to a complex problem of sustaining a safe environment for a vulnerable population of hundreds of minors and the personnel who support them (Sheikh, et al., 2025).

Proponents of facial recognition surveillance tout the benefits of biometric data collection and object identification data tracking (Prothero, 2023). In addition to surveillance for faceprint data, there are devices marketed to the K12 landscape which use artificial intelligence video collection to look for guns and other weapons. ZeroEyes, a platform which has expanded since several major school shootings, scans camera footage for over 300 types of weapons. The product suite detects weapons which are unsheathed, brandished, or unholstered (Singer, 2022). In addition to increasing an overall climate of perceived safety, proponents denote personalized access control with facial recognition validation and added security in high vulnerability areas such as mass gatherings for sports, concerts, or open house events (Stutzman & Davison, 2021). Security camera companies and some school districts have framed facial recognition technology as a powerful tool in preventing school shootings and saving lives, but there is little in terms of legislation which supports or mandates those protections (Tamez-Robledo, 2024). Despite a heavy dependence on this technology for day-to-day security measures, most school systems make the purchase, complete the installations, and make use of facial recognition surveillance devices without regard that even biometric data in infallible. The eye's iris, the face, a fingerprint, or a "handscape" can be reproduced, and in the era of deep fakes and artificial intelligence generated images, this flag in surveillance security may be more accessible and reproducible in the years to come (Stutzman & Davison, 2021). Facial matching is not 100 percent accurate even when using optimized data sets and advanced validation by humans to doublecheck machine-based matches (AWang, et al., 2024). With this fallibility in mind, Liu and Kahlil (2023) espoused safeguarding surveillance data for privacy should be ongoing with careful steps taken for protection.

Law and Policy Landscape

Surveillance tools bestow power on the watcher (Selinger & Hartzog, 2020). Biometric-based surveillance powered by artificial intelligence is implicitly different than any surveillance before, and with the innovations associated with this technology come new legal and regulatory challenges even though the concept of privacy is amorphous and still not finite in definition over 100 years after the Brandeis and Warren writing in *The Harvard Law Review* in the 1890s (Burrows, 2013). According to Korobenko, et al., (2024) high volumes of data collection and processing of facial recognition technology increase cybersecurity threats and possible misuse of biometric/facial recognition data. With no regulation, the start of biometric surveillance was without any kind of supervision or government oversight. In the 2000s, ClearviewAI scraped millions of faces from public websites, social media, and public forums. Armed with more face images than ever before, Clearview AI entered the arena of law enforcement, and their software is still the most widely used face matching technology in the world. Multiple mismatches and unlawful matches have resulted (Hill, 2024). ClearviewAI built millions of faces in a database used by law enforcement customers, and journalist Kashmir Hill brought to the forefront the lack of comprehensive facial recognition privacy laws as she uncovered multiple cases of mistaken identity in law enforcement

cases in the United States (Hill, 2024). According to the latest estimates, ClearviewAI's facial databases have over three billion images, and ClearviewAI's technology is used by most private entities including surveillance camera companies to give customers facial databases for validation and checking (Koenig, 2020; Hill, 2024).

Biometric surveillance is common around the world (Koenig, 2020). In the European Union, there is now an artificial intelligence act, which is that union of nations' first comprehensive artificial intelligence law, but even that act does not cover the rapidly evolving technology and the technology's effect on privacy and security (Korobenko, et al., 2024). In the United States, there is no comprehensive biometric privacy or regulation law. The United States has several major federal laws which were passed in the late 1990s and early 2000s to regulate and protection children in their internet actions. These are the Children's Internet Protection Act (CIPA) which may not protect the subjects of surveillance since the law was intended to keep inappropriate content from children, and the COPPA Act, the Children's Online Privacy Protection Act, which keeps children's identifiable information protected or impossible to collect before the child reaches the age of thirteen. Neither act, according to legal scholars, is going to protect the student who is surveilled using biometric facial recognition technology in the school setting (Chambers, 2022). The state laws governing student surveillance using facial recognition are varied. New York law prohibits biometric data collection of all kinds while New Hampshire, Delaware, Maine, Kansas, and South Dakota require consent for any hidden cameras. In California, all parties on camera must consent to be on camera, and two laws that stand out are the Illinois Biometric Privacy Act Law (BIPA), first passed in 2008 and amended in 2024, which dictates all parties must consent to be on camera. Municipal ordinances are even more varied. Some municipalities have put into ordinance that certain public areas must be under surveillance (Wang, X. et al., 2024). San Francisco in 2006, often on the forefront for innovation, limited the usage of surveillance technology (Wang, X. et al., 2024). Portland, Oregon municipal ordinance explicitly forbids collection of facial recognition data or even usage of biometric data collection in common city settings (Tamez-Robledo, 2024).

There is a spectrum of laws for surveillance, and there is a small number of laws for surveillance in schools, most of those are reactionary, but not comprehensive after specific school violence incidents, and very few of these laws address facial databases and their usage (Tamez-Robledo, 2024). As with many technology applications, the law often lags behind innovation. An existing legacy of scraped facial databases which have not been validated in many cases proliferates due to the ClearviewAI dominance in the marketplace (Hill, 2024), there are state legislatures which are indifferent or reluctant to act until there is marked social outcry or the impact on society is too great to ignore (Selinger & Hartzog, 2020). With spotty acts and regulations, technology in schools, specifically biometric surveillance, has not faced rigorous scrutiny or expanded regulation from policymakers even as technology's scope and use has expanded (Chanenson, et al., 2023). After the Marjory Stoneman Douglas High School shooting in 2017, the Florida legislature overwhelmingly passed legislation mandating surveillance systems be used comprehensively throughout every private and public school in the State of Florida (Nair, 2024). Florida law calls for threat assessment teams, student tracking, and surveillance equipment. In contrast, the State of New York, after introduction of student facial tracking system for behavior and instructional engagement in various local school systems, took the step to ban facial recognition technology in schools altogether (Prothero, 2023). Reactions to these laws are mixed. There have been declarations that use of facial recognition technology in schools will erode individual privacy and "disproportionately burden people of color, women, people with disabilities, and gender non-conforming people" (Galligan, et al., 2020). At the federal level, the United States Government Accountability Office called for a federal framework to regulate surveillance with facial recognition technologies by government agencies, but this call was made five years ago, and no framework has been created for review (Wang, X. et al., 2024).

Scholars, policymakers, and the media, according to Nair (2024), acknowledge biometric surveillance can threaten privacy and set up a climate for more discrimination risks. School administrators may incur unforeseen legal liability in hastily adopted surveillance practices that function in possible violation of statues and judicial precedent to protect student privacy interests (Fedders, 2019). Along with a vacuum of laws at the state and local level, there is a plethora of mixed research results regarding the usage of biometric surveillance. According to Chambers (2022), the reality is no overwhelming consensus of research exists showing effectiveness of school target hardening by facial recognition surveillance. Some studies point to increased security while others point to a climate of distrust based on student and staff interviews and surveys (Garon, 2021). The New York Law along with the Gerald R. Ford School of Public Policy Report from the University of Michigan point to a growing movement made by students, civil rights advocates, and technologists who see artificial intelligence-powered facial recognition surveillance as a dystopian addition which will cripple privacy due to exacerbating racism through disproportionate targeting or misidentifying (Galligan, et al., 2020; New York Office of Information Technology Services, 2023). The absence of comprehensive laws or litigation removes threats to vendors who are seeking to install thousands of cameras with steady paying monthly subscriptions in the K12 school setting, and this also means there is a "free-for-all feast" for surveillance data (Almeida et al., 2021, p. 385).

Student and Staff Surveillance Practices

Ho, et al., (2014) emphasized the dangers of constant surveillance for young people and people with disabilities. The researchers proclaimed surveillance, by its nature, can make the subject of that surveillance feel demeaned when what they consider to be their personal space is penetrated. Ho, et al., (2014) declared constant surveillance may even hinder or paralyze maturation due to surveillance's effect on trust. Yet there are others who point to disclosure and consent as the missing elements for most school surveillance using facial recognition technology (Selinger & Hartzog, 2020). There are calls for consent in many fields – not just education. Healthcare ethicists are advocating for facial recognition consent by those watched (Martinez-Martin, 2019). With the concepts of consent and disclosure, legal scholars point to this as the possible answer to the widespread usage of this technology. In an environment in which children are just learning to read, write, and other fundamental schools, self-disclosure and consent for minors are not ethical, and this means parents must be the consenting guardians who allow for the footage of their children, regardless of the child's behavior history, cultural differences, or disabilities (Alim, et al., 2017; Ebsary, 2018). Some proponents point out students are surveilled in public settings such as restaurants, playgrounds, concert venues, and other establishments, so surveilling at school should be treated as commonplace without the need for consent or disclosure (Ebsary, 2018). In fact, major manufacturers like Cisco, Avigilon, and others have touted their surveillance systems as avenues for monitoring students and their actions without disrupting the class with an additional adult presence (Avigilon, n. d.) Overall, many tools, including facial recognition surveillance cameras, often leave stakeholders unaware of the extent to which a child's information may be collected, repurposed, or even disclosed to third parties for non-educational purposes such as targeted advertising or profiling (Berson, et al., 2025). Disclosure to third parties is advised for those who are subject to surveillance, and the student handbook, the tool used to communicate expectations, regulations, and pertinent laws, is a possible mechanism for communicating these disclosures (Selinger & Hartzog, 2020). This is despite some vendor declarations that the more familiar and beneficial a surveillance tool seems, the easier it is to create a climate of acceptance without specific disclosures (Ebsary, 2018).

Students and Staff Handbooks

Handbooks for personnel and handbooks for students and their families cover a variety of topics. The hours of the school day, the logistics of drop off and pick up, the procedures for meals, and the dress code are all

usually covered. Handbooks usually provide guidance regarding behavior and consequences of unacceptable behavior. Handbooks are often filled with regulations and state or federal required language of notice and disclosure; however, handbooks are not uniform in concept or topic coverage. Many of them are tailored to the age of the student served or the type of employee, contracted or at-will. In today's age, most handbooks are online for public perusal. Handbooks are not always comprehensive, but they should contain parent/guardian "need to know" information, and handbooks for employees should contain legal disclosure and "need to know" information as well (Selinger & Hartzog, 2020, p. 115).

Handbooks are an avenue to make sure parents/guardians, visitors, administrators, school personnel, and students are aware of the means used to watch their activities and the happenings of their school (Berson, et al., 2025) These are tools which could be used to notify parents and guardians as well as employees of surveillance; however, there is a new factor which may be considered as administrators write handbooks in the years to come (Citron, 2024). New instructional tools are coming to market which utilize facial recognition, facial patterns, and facial expressions to determine student engagement and student learning activities. These facial recognition tools are being marketed to administrators and classroom teachers as teaching aids to determine which students are paying attention, which students are engaged, and how well the students are mastering the content (Banzon, et al., 2023). Disclosure for surveillance may be too late, but the disclosure for learning tracking is on the cusp of establishment.

Research Questions and Methodology

The comprehensive deployment of surveillance systems with facial recognition technology in K12 schools has outpaced policy development, creating a critical gap in institutional transparency and stakeholder protection. This study examines whether K-12 institutions adequately disclose biometric data collection practices to stakeholders through formal policy documentation.

Research Questions

RQ1: To what extent do K12 school handbooks disclose surveillance data collection, specifically facial recognition biometric data collection policies to stakeholders?
RQ2: How does biometric data policy disclosure vary among K12 personnel handbooks and K12 student handbooks based on demographic, geographic, and type of school (elementary, middle, high)?

Methodology

This study employed a systematic content analysis approach to examine biometric data policy disclosure in K-12 educational institutions. The research analyzed 325 publicly available handbooks, comprising 47 employee handbooks and 278 student handbooks from elementary, middle, and high school levels. All handbooks were accessed through official school district websites to ensure authenticity and public accessibility.

A standardized keyword search protocol was implemented across all documents using identical search terms including "biometric," "facial recognition," "face tracking," and other related terms. This uniform search strategy ensured consistent data collection and eliminated variability in search procedures. Each handbook underwent comprehensive digital text searching to identify any policy language addressing biometric data collection, facial recognition technology, or related surveillance practices.

The sample included diverse district types to ensure representativeness across the K-12 educational landscape. All documents analyzed were publicly accessible policy materials, representing official institutional communications to stakeholders. This methodology provided systematic coverage of formal

policy disclosure practices while maintaining consistency in data collection procedures across the entire sample.

The study analyzed handbooks from 278 public schools across a Southeastern United States state, representing diverse educational levels and community types. The sample included 145 elementary schools (52.2%), 100 middle schools (36.0%), and 33 high schools (11.9%), providing comprehensive coverage across K-12 educational levels. Geographic distribution encompassed 67 urban schools (24.1%) and 211 rural or suburban schools (75.9%), ensuring representation from farming communities, small towns, and metropolitan areas. This diverse sampling strategy captured significant demographic and socioeconomic variation, ranging from agricultural communities to major urban centers, thereby enhancing the generalizability of findings within the state's public education system. The inclusion of schools serving varied community types strengthens the study's ability to identify patterns in policy disclosure practices across different institutional contexts and stakeholder populations.

Findings

The systematic content analysis of 325 K-12 handbooks revealed a complete absence of biometric data collection policies across all documents examined. Zero instances of the search terms "biometric," "face," "facial recognition," "face tracking," "face authentication," “surveillance,” “camera,” “security camera(s),” or "biometric authentication" were identified in any of the 47 employee handbooks.

While 24 handbooks (7.4%) contained general surveillance camera disclosure statements, none of the 278 student handbooks addressed the biometric capabilities of these systems. The 24 surveillance disclosures typically included basic information about camera placement and usage for disciplinary purposes. For example, one handbook stated: "Portions of all campuses and buses are equipped with digital video cameras. Occasionally, video segments are used in student disciplinary investigations (Monroe County Schools Monroe County Middle School Handbook, 2025).” However, these statements made no reference to facial recognition capabilities, biometric data collection, or related analytical functions that may be embedded in modern surveillance systems.

The absence of biometric-specific policy language was universal across the diverse sample, indicating the lack of biometric data disclosure transcends individual district characteristics or administrative practices. Even districts that acknowledged general surveillance practices failed to address the advanced analytical capabilities of contemporary camera systems.

These results establish a critical distinction between basic surveillance transparency and biometric data collection disclosure. While some institutions provide minimal information about camera usage, none addressed the sophisticated biometric analysis capabilities that major surveillance manufacturers now include as standard features.

Discussion

The findings of this study provide valuable insights regarding the primary research questions while revealing significant governance gaps in K-12 educational institutions. Regarding the extent to which K-12 public school handbooks disclose biometric data collection policies to stakeholders, the results demonstrate a complete absence of such disclosure across 325 handbooks examined. This policy void indicates stakeholders such as students, parents, and employees often receive no formal notification about potential biometric data collection capabilities embedded in institutional surveillance systems.

The second research question examining variation in biometric data policy disclosure across different K-12 district characteristics reveals a troubling consistency: the absence of disclosure transcends district size, geographic location within the state, and institutional level as elementary, middle, and high handbooks were reviewed. Additionally, personnel handbooks were reviewed. All of the handbooks reviewed represented a variety of low income, medium, and high income communities of varying sizes with rural, suburban, and urban in the mix of handbooks. Whether elementary, middle, or high school settings, whether rural or urban districts, the pattern remains unchanged—no biometric data policies exist in standard, formal stakeholder communications of handbooks published on public websites.

These findings are particularly concerning given the widespread availability of facial recognition capabilities in modern surveillance systems. As documented in current literature, major camera manufacturers serving the K-12 market now include facial recognition and biometric analysis as standard features in their educational security offerings (Sheikh, et al., 2025). The disconnect between technological capability and policy transparency creates a scenario where biometric data collection may occur without stakeholder awareness or informed consent (Chambers, 2022).

The 7.4% of handbooks that acknowledged general surveillance camera usage further highlights this transparency gap. Districts demonstrate awareness of disclosure obligations for basic surveillance yet fail to address the sophisticated analytical capabilities these same systems possess. This selective transparency suggests either institutional unfamiliarity with modern surveillance technology capabilities or deliberate omission of biometric functionality information.

This policy vacuum occurs within a regulatory landscape where stakeholder protection remains inconsistent. While states like New York have enacted comprehensive bans on facial recognition technology in schools, most jurisdictions lack specific protections for students and educational employees regarding biometric data collection. The absence of both regulatory requirements and voluntary institutional disclosure creates an environment where biometric surveillance may expand without stakeholder knowledge or meaningful oversight (Chambers, 2022, Wang, X. et al., 2024).

Limitations

Several limitations should be acknowledged in interpreting these findings. This study focused exclusively on public schools within a single Southeastern United States state, which may limit generalizability to other regions with different regulatory environments or cultural attitudes toward privacy and surveillance. The analysis did not include private schools, which may operate under different governance structures and disclosure practices. Additionally, this research examined only formal handbook policies and did not investigate whether biometric data collection disclosure might occur through alternative communication channels such as enrollment materials, technology acceptable use policies, or separate privacy notices.

Furthermore, the study's focus on K-12 institutions exclusively identifies a need for similar research in post-secondary educational settings, where different stakeholder relationships and regulatory frameworks may produce varying disclosure practices. Finally, this analysis captured policy documentation at a specific point in time and may not reflect recent policy developments or ongoing institutional discussions about biometric technology governance.

Recommendations and Conclusion

This systematic analysis of K-12 handbook policies reveals a substantial gap between institutional surveillance capabilities and stakeholder transparency practices. The absence of biometric data collection policies across 325 public school handbooks represents an opportunity for enhanced governance rather than

institutional failure. Educational administrators face the challenging responsibility of balancing student and staff safety with privacy protection and transparency obligations, often while navigating rapidly evolving technology capabilities and limited regulatory guidance. Despite increased use of biometric tools for surveillance, administration, and instruction, the schools are not disclosing the possible use of this technology. Additionally, despite recurring emphasis in peer-reviewed literature and books on surveillance, the technology's storage methods are not being disclosed to surveillance subjects or software targets (Hill, 2024).

The findings should not diminish recognition of administrators' legitimate safety concerns and their commitment to protecting educational communities (LoSardo, 2020). School leaders operate in an environment where security threats require proactive responses, and surveillance technologies offer valuable tools for maintaining campus safety. However, the deployment of systems with biometric capabilities without corresponding policy frameworks creates unintended risks for both institutions and stakeholders.

Educational institutions can address these transparency gaps through several practical approaches. First, districts should conduct technology audits to identify current surveillance system capabilities, including any facial recognition or biometric analysis functions embedded in existing equipment (Kwid, et al., 2024). This assessment enables informed policy development based on actual technological capabilities rather than basic camera descriptions (Zeide, 2025).

Second, handbook policies should explicitly address surveillance technology capabilities beyond basic camera placement. Clear language informing stakeholders about potential biometric data collection, storage procedures, and usage limitations provides necessary transparency while maintaining administrative flexibility for safety purposes. Model policy language should distinguish between general surveillance monitoring and biometric data analysis capabilities.

Third, institutions should establish stakeholder notification procedures with respect for both safety requirements and privacy concerns. This might include annual technology capability updates, opt-out procedures where legally permissible and logistically possible, and clear data retention and sharing protocols. Such approaches acknowledge legitimate safety needs while honoring stakeholder rights to understand institutional practices (Wang, G. et al., 2022).

Finally, professional development opportunities for administrators, specifically school leaders, and technology leaders, should include education technology governance training to address privacy, consent, and disclosure requirements (Vavekenand, 2024). Many policy gaps may stem from limited awareness of modern surveillance capabilities rather than deliberate transparency avoidance (Weinstein, 2020).

Implications

These recommendations support rather than constrain administrative safety efforts by providing clear frameworks for technology deployment. With more features coming to surveillance cameras as artificial intelligence progresses, these procedures will put into place a foundation for disclosure. Transparent biometric data policies protect institutions from potential legal challenges while maintaining stakeholder trust, and that trust is essential for effective educational environments (Crawford, 2019). Proactive policy development positions districts to adapt responsibly to emerging technologies and evolving regulatory requirements in the face of new types of litigation and regulatory opportunities (Sullivan, 2019).

State and federal policymakers should consider developing model disclosure frameworks that balance institutional autonomy with stakeholder protection (Mattioli & Cabitza, 2024). Such guidance would

support local administrators in navigating complex technology decisions while ensuring consistent transparency standards across educational settings (Prinsloo, et al., 2023).

Ultimately, this research identifies an opportunity for the education community to lead in responsible surveillance technology governance. By developing comprehensive transparency policies that acknowledge both safety imperatives and privacy rights, K-12 institutions can model effective technology stewardship while maintaining their primary focus on educational excellence and community safety.

References

Addington, L. (2018). The use of visible security measures in public schools: A review to summarize current literature and guide future research. *American University School of Public Affairs Research Paper*, (3240204).

Akgun, S., & Greenhow, C. (2022). Artificial intelligence in education: Addressing ethical challenges in K-12 settings. *AI and Ethics*, *2*(3), 431-440.

Alim, F., Cardozo, N., Gebhart, G., Gullo, K., & Kalia, A. (2017). Spying on Students: School Issued-Devices and Student Privacy.

Almeida, D., Shmarko, K., & Lomas, E. (2022). The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks. *AI and Ethics*, *2*(3), 377-387.

Avigilon. (n.d.). *School Safety Solutions and Technology for secure campuses*. Avigilon. https://www.avigilon.com/industry/education

Banzon, A. M., Beever, J., & Taub, M. (2024). Facial Expression Recognition in Classrooms: Ethical Considerations and Proposed Guidelines for Affect Detection in Educational Settings. *IEEE Transactions on Affective Computing*, *17*, 93–104. https://doi.org/10.1109/TAFFC.2023.3275624

Berson, I.R., Berson, M.J. & Luo, W. Innovating responsibly: ethical considerations for AI in early childhood education. *AI Brain Child* **1**, 2 (2025). https://doi.org/10.1007/s44436-025-00003-5

Burrows, L. (2013, July 24). *To be let alone: Brandeis Foresaw Privacy Problems*. BrandeisNOW. https://www.brandeis.edu/now/2013/july/privacy.html

Chambers, D. (2022). How school security measures harm schools and their students. *Educational theory*, *72*(2), 123-153.

Chanenson, J., Sloane, B., Rajan, N., Morril, A., Chee, J., Huang, D. Y., & Chetty, M. (2023, April). Uncovering privacy and security challenges in K-12 schools. In *Proceedings of the 2023 CHI (Human Factors in Computing Systems) Conference on Human Factors in Computing Systems* (pp. 1-28).

Cisco Meraki. (2024, March 25). *Cisco Meraki Supports K12 Education*. https://meraki.cisco.com/industries/primary-education/

Citron, D. K. (2024). The surveilled student. *Stanford Law Review*, *76*, 1439.

Crawford, K. (2019). Halt the use of facial-recognition technology until it is regulated. *Nature*, *572*(7771), 565-566.

Ebsary, N. J. (2018). Biometric Monitoring Using Facial Recognition, Data Collection, and Storage: Safety and Privacy Perceptions of High School Students. *Journal of Computer Science and Systems Biology 11*(6), 313-318.

Fedders, B. (2018). The constant and expanding classroom: Surveillance in K-12 public schools. *NCL Review*, *97*, 1673.

Galligan, C., Rosenfeld, H., Kleinman, M., & Parthasarathy, S. (2020). *Cameras in the classroom: Facial recognition technology in schools*. https://dx.doi.org/10.7302/21934

Garon, J. M. (2021). To Be Seen but Not Heard: How the Internet's Negative Impact on Minors' Constitutional Right to Privacy, Speech, and Autonomy Creates a Need for Empathy-by-Design. *Mercer Law Review*, *73*, 463.

Hill, K. (2024). *Your face belongs to us: A tale of ai, a secretive startup, and the end of privacy*. Random House.

Koenig, R. (2020, January 22). *New Advocacy Campaign calls for banning facial recognition on college campuses - Edsurge News*. EdSurge. https://www.edsurge.com/news/2020-01-22-new-advocacy-campaign-calls-for-banning-facial-recognition-on-college-campuses

Korobenko, D., Nikiforova, A., & Sharma, R. (2024, June). Towards a privacy and security-aware framework for ethical AI: Guiding the development and assessment of AI systems. In *Proceedings of the 25th Annual International Conference on Digital Government Research* (pp. 740-753).

Kwid, G., Sarty, N., & Yang, D. (2024). A Review of AI tools: definitions, functions, and applications for K-12 education. *AI, Computer Science and Robotics Technology*.

Liu, Q., & Khalil, M. (2023). Understanding privacy and data protection issues in learning analytics using a systematic review. *British Journal of Educational Technology*, *54*(6), 1715-1747.

Lyu, G., Spero, M., & Henderson, C. (2024, December 28). *Facial Recognition Technologies*. The Regulatory Review. https://www.theregreview.org/2024/12/28/seminar-facial-recognition-technologies/

LoSardo, A. (2020). Faceoff: the fight for privacy in American public schools in the wake of facial recognition technology. *Seton Hall Legal Journal.*, *44*, 373.

Mattioli, M., & Cabitza, F. (2024). Not in my face: Challenges and ethical considerations in automatic face emotion recognition technology. *Machine Learning and Knowledge Extraction*, *6*(4), 2201-2231.

Martinez-Martin, N. (2019). What are important ethical implications of using facial recognition technology in health care?. *American Medical Association journal of ethics*, *21*(2), E180.

Monroe County Middle School Handbook (2025) Monroe County Schools 25 Brooklyn Avenue Forsyth, Georgia 31029. https://mcms.monroe.k12.ga.us/o/mcms/page/mcms-student-handbook

Nair, P. (2024). Surveilling Disability, Harming Integration. *Columbia Law Review*, *124*(1), 197-271.

New York , Office of Information Technology Services (2023). *Use of biometric identifying technology in schools*. Use of Biometric Identifying Technology in Schools. https://its.ny.gov/system/files/documents/2023/08/biometrics-report-final-2023.pdf\

Prinsloo, P., Slade, S., & Khalil, M. (2023). Multimodal learning analytics—In-between student privacy and encroachment: A systematic review. *British Journal of Educational Technology*, *54*(6), 1566–1586. https://doi.org/10.1111/bjet.13373.

Prothero, A. (2023, October 16). *Does facial recognition technology make schools safer? what educators need to know*. Education Week. https://www.edweek.org/leadership/does-facial-recognition-technology-make-schools-safer-what-educators-need-to-know/2023/10.

Selinger, E., & Hartzog, W. (2020). The inconsentability of facial surveillance. *Loyola Law Review.*, *66*, 33.

Sheikh, S., Stolberg, A., & Gilmour, A. F. (2024). Investigating advanced school surveillance practices and disproportionality: A systematic review. *Urban Education*, 00420859241279446.

Singer, N. (2022, June 26). *Schools are spending billions on high-tech defense for mass shooting*. The New York Times. https://www.nytimes.com/2022/06/26/business/school-safety-technology.html

Stutzman, B. T., & Davison, C. B. (2021). Privacy Issues Concerning Biometrics in Grades K-12. *Career Technical Education (CTE) Journal*, *9*(1).

Sullivan, E. T. (2019, January 31). *With safety in mind, schools turn to facial recognition technology. but at what cost? - Edsurge News*. EdSurge. https://www.edsurge.com/news/2019-01-31-with-safety-in-mind-schools-turn-to-facial-recognition-technology-but-at-what-cost

Tamez-Robledo, N. (2024, December 5). *Does facial recognition belong in schools? it depends who you ask - Edsurge News*. EdSurge. https://www.edsurge.com/news/2024-12-05-does-facial-recognition-belong-in-schools-it-depends-who-you-ask

Vavekanand, R. (2024). Impact of artificial intelligence on students and ethical considerations in education. *SSRN Electronic Journal*, 1-10.

Verkada. (n.d.). Verkada Education Surveillance. https://www.verkada.com/security-cameras/education/

Wang, A., Kapoor, S., Barocas, S., & Narayanan, A. (2024). Against predictive optimization: on the legitimacy of decision-making algorithms that optimize predictive accuracy. *ACM Journal on Responsible Computing*, *1*(1), 1-45.

Wang, G., Zhao, J., Van Kleek, M., & Shadbolt, N. (2022, April). Informing age-appropriate ai: Examining principles and practices of ai for children. In *Proceedings of the 2022 CHI conference on human factors in computing systems* (pp. 1-29).

Wang, X., Wu, Y. C., Zhou, M., & Fu, H. (2024). Beyond surveillance: privacy, ethics, and regulations in face recognition technology. *Frontiers in big data*, *7*, 1337465.

Weinstein, M. (2020). School Surveillance: The Students' Rights Implications of Artificial Intelligence as K-12 School Security. *North Carolina Law Review*, *98*(2), 437–479.

Zeide, E. (2025). Student Privacy's Student Neglect: Toward a Student-Centric Paradigm. *George Washington Law Review*, *93*(3), 535–609.