“Surveillance… n. close observation, esp. of a suspected person” [emphasis added]

--Reader’s Digest Oxford Complete Wordfinder, 1996

In 1995, “The total number of crimes committed per year in or near the 85,000 U.S. public schools has been estimated at around 3 million” (Volokh & Snell, 1998). Our educational system is evolving all the time, and one factor that is constantly changing is the aggressiveness within our schools. In 1940, a survey of teachers revealed that the biggest behavioral problems they had from students were “talking out of turn, chewing gum, making noise, running in the halls, cutting in line, [violating] the dress code, [and] littering” (Volokh & Snell, 1998). In 1990, the top-rated problems were “drug abuse, alcohol abuse, pregnancy, suicide, rape, robbery, [and] assault” (Volokh & Snell, 1998). In 1940, we had little need for surveillance beyond a teacher’s observation and intervention. Today, however, we live in a much more diverse society with troubled youth and adults who have easy access to weapons, drugs, pornography, etc., which have enabled students and staff to bring their violent and/or inappropriate tendencies into the naïve schools. What worked in 1940 (teacher-student confrontation) is not as realistic in
contemporary schools, where teachers are hesitant to confront misbehaving students due to fear of violent retribution (Volokh & Snell, 1998) and where teachers are sometimes involved in inappropriate activity themselves during school hours.

Over the past few years, though, schools have begun experimenting with different types of surveillance in an effort to decrease such inappropriate activity by the students and staff. Since 1995, the percentage of victimized students dropped from 10 percent of all students to 6 percent in 2001 (U.S. Dept. of Justice, 2002). What contributed to that change? It was not just one method, but rather a collaboration of multiple surveillance techniques, including school-management-based programs, environmental modification, and educational and curriculum-based programs (Volokh & Snell, 1998). This project addresses the value of a few different types of surveillance in schools, including supervision and observation through cameras, metal detectors, locker searches, and Internet tracking (email and web searches) and offers recommendations for their limited use. Not specifically or thoroughly discussed in this project are profiling and violence-prevention programs—mainly due to the limited time we had to work on this project and the broadness of those topics.

To read more about the specific security measures and how they should be used in schools, please click on the links below:

Security Cameras


Project Creator Contact Information:

**Kathy Davis, John Kelsey, Dia Langellier, Misty Mapes, and Jeff Rosendahl**

Course - **EPS 313**

**CTER** program at **UIUC**

Course Instructor - **Nicholas Burbules**
Surveillance in Schools: Safety vs. Personal Privacy

Security Cameras

Introduction

In recent years, violent episodes in schools in Arkansas, Colorado, California, Kentucky, Mississippi and other states have led educators and legislators to make "Safe Schools" a priority. Like many issues in education, suggestions on how to make a school "safe" have proceeded simultaneously on many different tracks. Teaching students strategies they can use to combat emotionally explosive situations through initiatives such as character education and peer mediation is one track that is currently used to help make schools safer. Another method that many schools are pursuing is stationing a full-time security officer (or officers) in the building. One of the most controversial methods involves surveillance of students through video cameras.

What are Security Cameras?

School video surveillance systems consist of cameras placed in areas where they can monitor activity as it takes place. These cameras may include features like pan, tilt, and zoom; may be placed in outdoor or indoor locations; and may include infrared recording options (technical discussions from Green, 1999, Video camera table of contents). Most cameras are used with recording systems, either VCR's or digital recorders. Using a digital recorder is the preferred option for easy storage, easy recall, and easy viewing over different monitors (discussion of strengths and weaknesses of different recording mediums from Green, 1999, Video recording table of contents).

One of the most popular video surveillance tools for schools is the SecureView system, manufactured by View Systems Inc., Englewood, CO.
The system transmits images from cameras to a digital hard drive storage system. Output can be seen on a monitor that displays four frames of video (each takes up a quarter of the screen), or on desktop computer monitors, which are networked to receive video feeds from the cameras. The system allows users to quickly view a recorded video based on search criteria (Adams, 2001).

Another similar system is Sensormatics, which combines different types of cameras with monitors, video servers, and multiplexers to offer schools the same recording, storage, and playback functionality (SecuritySupplyHouse.com).

**Benefits**

At this time there are no unbiased studies of the benefits and drawbacks of the use of video surveillance systems in schools. Naturally, proponents of using these systems emphasize the benefits, while opponents discuss the drawbacks. Benefits to using cameras depend on the individual school and the problems it faces. Experts recommend following a procedure that first determines the problem, then decides how surveillance equipment can be used to address the problem (School security...) (Green, 1999, Chapter 1, A systematic approach).

One of the advantages that proponents of video surveillance claim is peace of mind for students and staff (Green, 1999, Why video cameras?). "Security experts and administrators who use the cameras say students and teachers seem to appreciate the increased sense of security" (Hafner, ¶ 9). Naturally this is one of the most important features of a system that schools use in response to recent highly-publicized incidents of violence in the schools. Green argues that although cameras are passive, information about their presence will make its way through the community. Students and staff feel safer knowing that potential perpetrators will be scared off by the presence of cameras before committing an offense.

Another advantage that can be measured is a reduction in property damages such as vandalism and theft (Ballenas...) ("The witness"...). "Far too often the administration can only react to vandalism with time-consuming, seldom successful and often fruitless attempts to identify the perpetrators" (Ballenas..., ¶ 3). "The costs [of theft] are monetary (no money for
replacement) and inconvenience (educational opportunity loss for our students)" (Ballenas..., ¶ 4). Video surveillance systems provide a solution for these issues. "Cameras certainly multiply security's eyes, helping the administration to apprehend and discipline students caught on camera" (Sauvain, 2002, ¶ 3). Cameras also provide security in hidden areas of schools that are physically difficult to monitor (Schneider, 2001).

Finally, schools using video surveillance claim better behavior because of monitoring. "Sometimes just the idea in kids' minds that there's a camera recording them keeps them from causing trouble or being difficult" (Gross, as quoted in Baxter, 2003, ¶ 14). "Word gets out (about the cameras and searches) and I think it's had an effect that way" (Pfeffer, quoted in Oakes, 2000, ¶ 8). Some schools view cameras as having a dual purpose. "All of Bullitt County's buses are being equipped with cameras to randomly monitor student behavior and driver performance" (Baxter, 2003, picture caption). Since stored video records provide tangible evidence, school officials may find employee performance evaluations easier to do using video surveillance tools than face-to-face. The use of video records as evidence and as a means of identification may also be a reason students may be less inclined to cause trouble (Adams, 2001) (Schneider, 2001). "The solid documentation that a video recording provides can be invaluable in situations involving liability claims" (Green, 1999, Why video cameras?).

**Drawbacks**

Opponents to using video surveillance systems in schools emphasize several major drawbacks that need to be considered when studying the implementation of this kind of system. Cost is an obvious consideration. The equipment, testing, and installation of a system in a single school could cost $30,000 or more (Green, 1999, Why not video cameras?) (Sauvain, 2002) (Hafner, ¶ 10). Further, the school will have to provide money in future budgets for maintaining and upgrading the equipment (Schneider, 2001).

Equally important is the question of effectiveness. "Will it let an administrator know who did what? Sure,' said William Behre, an assistant professor at the College of New Jersey's Department of Special Education. 'Will it stop violence in any significant way? I don't think so.' He also noted that Columbine High School used surveillance cameras" (Oakes, 2000, ¶ 7).
Behre was a researcher in a University of Michigan study that studied violence in Midwestern schools and how the school administration responded. Opponents to cameras claim that as passive control devices, they won't be as effective in preventing violence as an adult would be.

Another disturbing thought is that adults with access to the surveillance system will use it for profiling purposes. "What assurances can be made that a student will not be unfairly targeted for surveillance because of their race, sexual orientation, gender, appearance, or religious beliefs" (Sanfilippo, 2002, ¶ 10)? Students have the concern they will be individually tracked by school administration (Security cameras...). In The Four Problems With Public Video Surveillance, the American Civil Liberties Union urges "a consensus on limits for the capability of public CCTV systems" and "legally enforceable rules for the operation of such systems" (The four problems, Section 3 subheadings).

Finally, there is the question of how a surveillance system affects student morale. "When schools turn to technology as a 'quick fix,' there is a high risk of reinforcing a climate of fear and distrust, undermining the social ecology of the school, instead of actually having an impact on the identified problem" (Schneider, 2001, ¶ 33). "What's wrong with the school? Have they lost the trust in their own students to a point that they have to spy on their lives" (Security cameras..., Con column, ¶ 2)? "There's no indication that there's a need for this kind of prison-style security. The message it sends to students is 'We don't trust you, and everybody is a suspect'" (Golden, as quoted in ACLU protests..., ¶ 6). "The more restrictions schools impose on students, the more alienated students are likely to feel, and the less involved in the learning process" (ACLU urges..., ¶ 5). "The cameras are teaching that government can and will invade your private space" (Willis, as quoted in Virginia school..., ¶ 11). "Heavy-handed school search policies foster distrust between students and administrators. An encounter pursuant to an expansive school search policy is likely to impress upon a student that he or she is inherently untrustworthy or that people who have authority may wield it without regard to individual liberties" (McIntyre, as quoted in Reutter, ¶ 5).

**Legal Questions**

Since laws concerning privacy issues, civil rights, and/or video surveillance vary widely, any school contemplating an electronic surveillance program
Surveillance - Security Cameras

should be sure to check with its school attorney prior to implementing the program. However, there are some general rules that seem applicable to most situations. Cameras cannot be used in areas of the school where staff or students have a "reasonable expectation of privacy" (Green, 1999, Legal aspects...). This would include private offices in addition to the obvious locations of restrooms and locker rooms. Conversely, cameras can be used in places where staff or students lack a reasonable expectation of privacy (Surveillance technology..., 2001). Examples include common areas like hallways, cafeterias, libraries, and parking lots. Recording audio conversations is seen to be a greater Fourth Amendment violation than video recordings at this time. "Whether the Fourth Amendment is implicated depends initially on whether the asserted search or seizure - for example, the electronic surveillance - infringes on a "reasonable expectation of privacy"" (Jenero & Mapes-Riordan, 1992, page 75, ¶ 2, italics are not original).

Since there are few case studies regarding the use of video surveillance in schools, a short examination of some of the existing business court cases may prove helpful. These don't apply exactly to a school situation, since most cases show the results of employee (as opposed to student) monitoring. There is no federal law that governs video surveillance, but several courts have ruled that employees have the right to be free of "surreptitious electronic surveillance" (9th circuit..., 2001, ¶ 1); employees have the "fundamental right to be free from surveillance" (Workplace privacy..., Section B-2 ¶ 3); and employees have a "reasonable expectation of privacy against disclosed, soundless video surveillance while toiling in open and undifferentiated work areas" (Workplace privacy..., Section B-2 ¶ 3). In Technological Surveillance in the Workplace, a paper written for a Colorado law firm, the author points out that just as surveillance of students in schools can result in low morale, so too can surveillance of employees. "Employee monitoring may be counterproductive by resulting in lower morale, increased job stress, and perhaps even lower production" (Johnson, 1995, Conclusion, ¶ 1).

Schools should also consider what kinds of activities cameras in "public" areas observe students engaging in. "The likelihood that the Fourth Amendment's protections will come into play increases in direct proportion to the extent to which the employer's surveillance infringes on an employee's personal conversations or activities inside or outside the workplace. As the surveillance moves away from strictly work-related matters of legitimate
interest to the employer, it necessarily moves into areas in which the employee has a heightened expectation of privacy" (Jenero & Mapes-Riordan, 1992, page 79, ¶ 4).

**Recommendation**

If a school is considering deploying a video surveillance system, officials should consider the following questions:

1. What specific security threats and concerns is the school attempting to address by using a particular type of security equipment?

2. How will this equipment help address these threats and how will the school actually use it on a day-to-day basis?

3. If the school is able to purchase the equipment, how will it be maintained, repaired and upgraded?

4. What might be the possible (or unintended) consequences of these security technologies? (School security...) (Schneider, 2001)

In addition, school officials should employ a cost-benefit analysis to compare investment in a video surveillance system with other alternatives to address the above questions, as well as addressing other school needs based on priorities. If the school decides to implement video surveillance cameras, officials should be sure to create a policy for use before purchasing and installing the equipment to eliminate any future confusion. A Connecticut school board found itself with installed cameras but an inadequate policy (Damon) when one member of the board questioned but an inadequate policy (Damon) when one member of the board questioned using the cameras 24 hours a day, 7 days a week. It was her understanding the cameras would only be turned on when school administration was not present. Now that the cameras are in constant use, she is concerned about violating student privacy. "'I feel bad we didn't think about it like Margaret has [before we put the cameras in],' said board vice chariman Vincent Saviano. 'It's hard to write a policy on it when we're not clear on what the applications of the cameras are going to be.'" (Damon, ¶ 6).

Since each situation is different, it is recommended that school officials, parents, students, teachers, and community members carefully consider the
above questions and the possible consequences. These systems can be useful in achieving limited objectives that are well defined and understood by all stakeholders in all stages of the planning, implementation, and assessment processes. Video surveillance can be used in conjunction with other methods of surveillance, including metal detectors, locker searches, and Internet/e-mail tracking. However, each of these other surveillance methods brings its own set of benefits and drawbacks, and schools trying to incorporate more than one method may find the situation too complicated to be effective. Although there are some strong arguments against the use of video surveillance in schools, a school that has a problem the system is effective in addressing (i.e. need to reduce property damage), a policy that clearly indicates to all stakeholders the purpose of the system, and data illustrating how the implementation of the system is the best use of available resources would do well to incorporate a video surveillance system at their school.

References


Project Creator Contact Information:
Kathy Davis, John Kelsey, Dia Langellier, Misty Mapes, and Jeff Rosendahl
Course - EPS 313
CTER program at UIUC
Course Instructor - Nicholas Burbules
Introduction

Surveillance through the use of metal detectors has become a controversial issue in many school districts. Some argue that metal detectors are intrusive, unconstitutional, ineffective, evasive, and unnecessary. Others argue that metal detectors are non-intrusive, efficient, and essential to create safer schools. Who is right? Actually, neither party is probably accurate since they both express such extremist views. Metal detectors, used responsibly, can be highly effective in preventing violence in schools. However, they do not work as a magic wand; they do not single-handedly eliminate violence in schools, and they do nothing to prevent violence outside of the schools. Still, if used in conjunction with other types of surveillance, such as video surveillance, locker and parking lot searches, Internet tracking, profiling, and violence-prevention programs, metal detectors work to provide a safer learning environment for our students. That is not to say that all schools need metal detectors or that metal detectors should be used to inspect every student every day. “The ideal violence-prevention policy will likely be different for each school…. [T]he only reasonable agenda for fighting school violence is to encourage individual schools to experiment and find what ‘works’ in their particular circumstances” (Volokh & Snell, 1998). Whether or not a school should use metal detectors for surveillance is a decision that should be made by school
officials. If they do decide to use this method, though, “governed by reasonable guidelines,” they will almost certainly find that the method is both effective and legal (Johnson, 2000).

What are Metal Detectors?

A metal detector is, simply, an electronic instrument used to locate specific types of metal. The capabilities of metal detectors vary according to the specific needs of the consumer. In addition to recreational purposes, metal detectors are used for airport and building security, event security, item recovery, archaeological exploration, and geological research (Tyson, 2003). Metal detectors also come in several physical styles--“beachcomber,” hand-held, and mounted styles can all be effective for their intended use.

“Beachcomber” metal detectors are designed to assist consumers in their quest for hidden treasures. They are lightweight but somewhat large and awkward if used for other purposes (such as security).

Hand-held detectors are smaller and less obtrusive than beachcomber detectors. They are also usually “powerful and sensitive enough to detect all concealed metal weapons, including the smallest knives and guns” (“Garrett,” n.d.; Tamiami, 2002).

Mounted, or walk-through, detectors are not small, but they are even less invasive than the others since the person and/or items to be inspected need only to pass through the detector without any close personal contact. These detectors have numerous sensors, each sensor’s sensitivity rate being set at the proper level to detect specific metals and eliminate interferences such as “x-ray devices, video monitors and communications equipment” (“Walk-Through,” n.d.). Mounted detectors are typically more expensive
than the others, but they are built to endure high traffic, hard weather, and rough handling ("Walk-Through," n.d.).

**Should Metal Detectors Be Used in Schools?**

**Overview of Violence in Schools: Is There a Need for Surveillance of Weapons in Schools?**

Unarguably, school violence is a problem that cannot be regarded as trivial. The problem of students bringing weapons to school is an issue that will not go away by itself. As acknowledged in the trial of People versus Pruitt in 1996, “Judges cannot ignore what everybody else knows: violence and the threat of violence are present in the public schools….School children are harming each other with regularity” (qtd. in Johnson, 2000). Obviously, this is not true in every school district, but the point being presented is that violence in schools must be eradicated.

Inner cities have the highest rate of violence reported. “The problems of urban schools are particularly acute and are complicated by their connection to the prevalence of poverty, crime, and despair in America’s cities” (Oneill, n.d.). More specifically, students in inner-city schools attended by “predominantly lower SES minority children” are two times as likely to be victimized through violence than students in suburban or rural schools ("Facts about Violence," 2000). In the early 1990s, over 50 students from Thomas Jefferson High School in Brooklyn were killed, some of the murders taking place at the school (Volokh & Snell, 1998). Many inner-city school districts have to deal with the issue of weapons in the school on a day-to-day basis. Seven years ago, 17 percent of inner-city schools reported at least one serious crime while only 8 percent of rural schools reported such an incident ("Another Take on School Violence," 1999). The schools with high crime rates have a
higher need for metal detectors than other schools, and they may feel the need to use metal detectors on a regular basis—maybe even everyday on every student—in order to maintain a safe learning environment for the students.

Still, violence exists at other school districts outside of the inner city. The famous Columbine High School tragedy in Littleton, Colorado, in April of 1999 and the shooting that took place at a high school in Conyers, an “upscale suburb of Atlanta, [Georgia],” in May of 1999 were two such incidents (Clark, 1999). These non-urban schools did not fit the stereotypical profile of a potentially violent institution because of their location, but the violence or potential for violence was there, nonetheless. These types of schools may find that metal detectors work effectively for them on an as-need basis, like in cases in which individualized suspicion arises.

It is also important to note that violence does not just occur at the high school level. Students and teachers alike become victims of violence in some elementary schools as well. According to the National Household Education Survey in 1993, 60 percent of elementary students and 77 percent of middle or junior high students reported the occurrence of victimization through robbery, bullying, or physical attack at school. In addition, 10 percent of elementary students and 12 percent of middle or junior high school children reported that they had been bullied; and four to five percent of elementary and junior high school children reported that they had been physically attacked (Mary Jo Nolin, Elizabeth Davies, and Kathryn Chandler of Student Victimization in School: Statistics in Brief, 1995, qtd. in Volokh & Snell, 1998). More recently, federal figures show that one in every ten students who were expelled in the 1998-99 school year for bringing a gun to school was an elementary student (Toppo, 2003). On February 29, 2000, at Buell Elementary School in
Mount Morris Township, Michigan, one six-year-old shot and killed another six-year-old student with a semi-automatic that he had brought to school (Buhrmann, 2000). Students are not the only victims either: "the percentage of elementary school teachers who said they were attacked rose from 4.9% to 5.5%" from 1993-94 school year to the 1999-2000 school year (Toppo, 2003). This horrible exposure to violence at such a young age is alarming, and some type of surveillance should be implemented to prevent it from occurring at school—for the sake of the students and the teachers.

A violent act here and there does not necessarily label an entire school district as “violent” though. Many of the incidents named above have become sensationalized because of the school’s history of non-violence, or at least its lack of serious violence. School officials need to consider many aspects of the district’s learning environment before grabbing up the latest surveillance technology to solve their problems, particularly if the school does not really even have a violence problem but rather just an isolated incident. “As Rutgers University criminologist Jackson Toby puts it, ‘everyday school violence is more predictable than the sensational incidents that get widespread media attention, because everyday school violence is caused at least in part by educational policies and procedures governing schools and by how those policies are implemented in individual schools” (qtd. in Volokh & Snell, 1998).

Still, we cannot ignore that 5 percent of 12th grade students have been “purposefully injured” and that 12 percent were threatened with injury by the use of a weapon while in school during the past twelve months (Johnson, 2000); and we certainly cannot ignore that nine percent of male high school students admit to having brought a weapon to school within the past 30 days or that three percent of high school seniors admit to bringing a gun to school.
within the past 30 days (Johnson, 2000). Statistics vary from school to school, but the fact is that violence is prevalent in many school districts throughout the nation, and each community needs to be aware of its own level of violence. Once a community determines the reality of violence in its school district, it needs to take action to arrest the violence and prevent it from recurring. One method that can be effective in curtailing the use of weapons in schools is surveillance through metal detectors.

**Benefits and Drawbacks: Do Metal Detectors Really Work?**

Some argue that metal detectors do not work. Michael Ferraraccio (1999) believes that the installation of metal detectors can actually be detrimental to a student’s learning experience, causing him/her to find the school buildings and the people in them dangerous. He poses the question, “Is the installation of metal detectors more likely to alleviate fear, or foster fear?” Others who believe that metal detectors are not effective base their arguments more on statistics of failure. For instance, David Marcus (1999) recalls an incident at Wilson High School in Washington, D.C., where “metal detectors couldn’t prevent a fatal stabbing just outside the building” in 1998. Another incident occurred in April of this year in the gymnasium at John McDonogh High School in New Orleans, where four teenagers opened fire, killing a 15-year-old boy and wounding three girls. “It was not immediately clear how the gun got through metal detectors and guards at the school. Students and school security officers said there was a hole in the fence near the gym” (“Gunmen Get Past…,” 2003).

Such incidents do occur, unfortunately, because metal detectors, used as the sole violence-prevention method, do not completely cure the disease of violence in schools. Metal detectors can do only what they profess to do: detect metal. Even so, many
students have found ways to bring weapons into schools, regardless of the surveillance through metal detectors. Education expert Mary Ann Raywid claims “she saw students intentionally play games where the goal was to hide things from security cameras, and shield knives and guns from metal detectors. The games even made kids who wouldn't be interested in bringing guns or knives to school compete just to see if they could ‘beat the machine’” (qtd. in Oakes, 2000). William Behre, an assistant professor at the College of New Jersey's Department of Special Education, who is studying violence in midwestern schools, said that “he has had students teach him personally how to get weapons past metal detectors” (Oakes, 2000).

However, they are effective in reducing violent crimes in schools. In 1992, the Green Pastures Center in Oklahoma discovered that the number of students bringing weapons to schools declined by more than half in just one year and that violent crimes and criminal trespass dropped by 35 percent. “[S]chool police attributed the decline to the presence of more metal detectors” (Volokh & Snell, 1998). Robert Johnson (2000) reports that the Chicago schools confiscated 15 guns and 294 weapons in 1991-92, 42 weapons in 1992-93, and four guns in both 1993-94 and 1994-95. “These data show that metal detectors work—they detect illegal weapons and aid their confiscation” (Johnson, 2000). More recently, the National School Safety Center reported that there was a 40 percent decrease of school-associated violent deaths in the 1998-99 school year from the previous school year (Jamison, 2002). And that was just one year’s progress.

Obviously, metal detectors have their limitations. No violence-prevention program is foolproof by itself: “No one knows how to foil a determined young killer. Nor does anyone confidently proclaim how to identify such a potential killer and then intervene to reform his character and cure his alienation” (Johnson, 2000).
However, when used in conjunction with other methods, metal detectors do drastically reduce the number of weapons in schools and prevent the recurrence of violence. The number of crimes committed on school grounds decreases continually. “Violent victimization rates for students varied from a high of 59 violent victimizations per 1,000 students in 1993 to a low of 26 per 1,000 students in 2000” (U.S. Dept. of Justice, 2002). Nobody claims that metal detectors are the only solution to solving the problem of crime in schools--“violence in schools is never 100 percent preventable but there are many tools including metal detectors that can cut down the chances” (Clark, 1999).

**Legalities: Do Metal Detectors Violate the Privacy Rights of Students?**

“The Fourth Amendment to the United States Constitution provides in part that ‘The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause’” (qtd. in Ferraraccio, 1999). Are students awarded this right too, or do they have more minimal expectation of privacy in schools, thus reducing their right to privacy, like patrons of an airport or courthouse, where surveillance of weapons through metal detectors is standard for everyone?

Would it be hypocritical to deny students a right to privacy? Some argue that metal detectors work contrarily to a school’s effort to teach humanistic progress and that they redefine a student’s body space due to the power of the state. Isn’t it the school’s mission, in fact, to prepare students for “social adjustment”? (Volokh & Snell, 1998). Michael Ferraraccio (1999) agrees: “it would be ironic to, on the one hand, educate students in the virtues of citizenship, while on the other hand
disregarding their constitutional rights.” Unfortunately, the question of hypocrisy is not easily answered, though. One must consider several issues, such as invasiveness of personal privacy, public safety, and court-declared legalities of metal detectors in schools.

**Issue 1: Invasiveness of Metal Detectors**

Although John Courtsunis (2001) implies that the metal detectors are no less intrusive than a strip search, there is no evidence of long-lasting ill effects on students who have been searched using minimal search tactics. A California court, upon reviewing the search policy of a high school using metal detectors, found the school’s random searches to be “minimally intrusive and reasonable under the circumstances” (Johnson, 2000).

One way to minimize the invasion of personal space is to buy a metal detector that “permits immediate searches to be made without touching the person” (“Garrett,” n.d.). In addition, metal detectors are becoming more accurate in detecting weapons without false alarms, leading to fewer unnecessary pat downs (Tamiami, 2002). In fact, the Garrett Hand Held Super Scanner boasts that it is “virtually eliminating the need for pat downs during weapons screenings, saving patrons from embarrassment” (“Garrett, n.d.). Also, many metal detectors come with earphones or vibrating alarms “for less conspicuous detecting” (“Garret,” n.d.).

**Issue 2: Public Safety vs. Personal Privacy**

Perry Zirkel (2000) expresses his concern that the lower courts are moving toward a “suspicion-less” standard for student searches, which require “at best, a particularized finding of pronounced school violence,…and at worst, only a public
perception…of a generalized threat to school safety.” School safety is definitely a concern, but how does one determine the level of necessity for the use of surveillance to maintain or to regain a safe learning environment? “The problem… is how to balance the state’s interest in maintaining a safe learning environment with the student’s interest in privacy” (Ferraraccio, 1999).

Obviously, not all schools need to use metal detectors every day. In schools with records of less violence, metal detectors should be used only upon reasonable suspicion…either of an individual person or of a specific incidence of threat to the school. For instance, if a school official has received a tip that a specific individual in the school has a weapon, then the school official should follow the policy procedures to search that one individual. If, however, a school official has received a tip that some undetermined person in the school has a weapon, then all persons within the school should be searched under policy procedures. In one such case, a bus driver noticed fresh slashes in a seat on the school bus, giving the school officials reason to suspect that somebody had a knife or other cutting instrument on school grounds. Because of the specific incident of threat, the metal detectors were used on all of the junior high and high school students, according to the school search policy (Ferraraccio, 1999).

Other schools with a higher frequency of violent crimes in their district may choose to use metal detectors every day on every person who enters the school grounds as a precautionary measure—to protect the students and staff from potential harm. Although students here have a lower expectation of privacy, they have a higher confidence of security within the schools. Courts have overwhelmingly supported the right of the schools to conduct routine searches because “the need to protect students
from weapons overrides the individual student’s right to privacy, and searches under such justifications do not constitutionally require that there be individualized suspicion” (Ferraraccio, 1999).

Although Ferraraccio (1999) concedes that metal detector searches are constitutional when suspicion arises, he cautions us that “the removal of individualized suspicion tends to further lower one’s expectation of privacy, so that as metal detector searches become more and more commonplace, the next generation of students will become even less sensitive to what should constitute a legitimate expectation of privacy, perhaps setting the precedent for even more intrusive searches, and less reasonable searches, than exist now.” However, Robert Johnson (2000) says that Ferraraccio “badly underestimates the importance of countervailing safety considerations.” The intention of the courts, after all, is not to remove the privacy of students but rather to ensure the safety of all.

The bottom line is that school officials understand their district’s personal needs better than those who have become biased in their opinions due to exposure of specific cultures and attitudes. The frequency of the use of metal detectors in schools is dependent upon the level of violence that those schools are exposed to. School administrators must have a “compelling interest to intrude upon the students’ reasonable expectation of privacy,” even if that compelling interest is the general safety of students and orderly environment “free of the possession and use of weapons” (“Use of Metal Detectors in the Schools,” n.d.). Whether the search is to be carried out on all students or on just individual students, suspicion of a weapon on campus must be an issue.

**Issue 3: Legality of Metal Detectors in Schools**
Courts have overwhelmingly determined that using metal detectors in schools is legal. In 1994, the government tried to enforce a policy nationwide that required schools to implement a safety program in their schools, offering metal detectors as one effective method (“U.S. Schools…,” 1997). Although the Supreme Court eventually overturned the requirements, the lower courts still support safety measures such as metal detectors in schools. In fact, they even support cases in which individualized suspicion is absent: “the courts have repeatedly approved the constitutionality of weapon-related suspicionless student searches conducted with metal detectors, and…these decisions are fully consistent with the school-related decisions of the United States Supreme Court” (Johnson, 2000). Even if they did not necessarily defend “suspicionless” searches, there is little that they can do to deny that right to the schools: “to say that a search may be ‘reasonable’ absent a warrant or probable cause is not to say much, for the Court has never defined or offered much in the way of a guideline as to what is meant by reasonable” (Ferraraccio, 1999). Regardless of the ethics of the issue, which could be discussed endlessly, the reality is that the courts support the schools’ decision to use metal detectors.

**Recommendations: How Searches Should Be Conducted**

Once school officials determine that the school district does in fact need metal detectors, they need to decide how they want to implement the surveillance program in the school. Will searches be performed on a daily basis? Will the searches be random? Will the searches be performed solely upon suspicion of an individual or isolated threat of violence? This decision needs to be considered very thoroughly. Although law is on the side of the school, ethics are on the side of the students, especially if there is no routine threat of violence in the school district. The implementation of such a program should be as minimally
intrusive as possible to protect the students’ right to personal privacy.

“One way of setting norms of behavior is to adopt a written policy clearly prohibiting certain activities, like bringing weapons or harassing other students” (Volokh & Snell, 1998). The policy should also address methods of searches for such weapons and consequences should weapons be discovered in a person’s possession.

First, everyone in the school should be told in advance that searches will take place upon suspicion or upon administrative decision, and everyone should be informed of the purpose of the search, most likely that it is to prevent weapons from being brought into the school. According to Shelby County School’s 2002-2003 Student-Parent Handbook (2002), one good way to inform school visitors as well as students and staff about the metal detector surveillance program is to post signs “notifying students and visitors that they are subject to unannounced electronic screening for weapons.” Not only is the information in the handbook for parents and students to see, but it is also available to all who enter the school.

Once a search is initiated, the officers conducting the search should maintain professionalism, following a uniform procedure, thus “safeguard[ing] the students from the discretion of those conducting the search” (Ferraraccio, 1999).

Whenever a person is screened due to individualized suspicion, that person should be brought into a private place, such as “the principal’s or associate principal’s office” (“Use of Metal Detectors in Schools,” n.d.) to create the least intrusive environment for the suspect. In addition, an adult besides the official implementing the search should be present (“Use of
Metal Detectors in Schools,” n.d.) to ensure and verify that no inappropriate action takes place during the search. Anything that occurs which is contradictory to the specific policy procedures should be reported to the superintendent for further investigation.

During the procedure, the suspect will first be asked to remove all metal objects in his/her possession before the metal detector is used in order to reduce the chance of a false alarm with the metal detector. After all volunteered metal objects have been exposed by the suspect, the official will scan the student’s body and possessions with the metal detector (either a hand-held or mounted model). Mounted models, although more expensive than hand-held models, are more effective and less intrusive, according to many (for example, Volokh & Snell, 1998, and Shelby County Schools, 2002). Suspects merely pass through them without any fear of being inappropriately touched by an official. Still, hand-held models can be highly effective and minimally intrusive as long as the official is careful to avoid body contact. If the metal detector is activated, the suspect should be asked once again to remove all remaining metal objects from his/her possession. The suspect is given the benefit of the doubt that the remaining metal was left on his/her possession unintentionally the first time s/he was asked to remove all metal objects; s/he is thereby given another opportunity to avoid the following, more intrusive steps of the procedure. The intention is not to harass a suspect, but to prevent unnecessary further intrusion. After all, a “metal detector triggered by car keys could give officials carte blanch authority to conduct a further and more intrusive search than can be justified by the purpose of the initial search” (Ferraraccio, 1999). After the suspect’s second attempt at removing all metal from his/her possession, the official scans the suspect’s body and possessions a second time. If the alarm is activated again, the suspect is subject to a “pat down,” whereupon a school official of the same gender (as supported by many
articles, including Ferraraccio’s “Metal Detectors in the Public Schools: Fourth Amendment Concerns,” 1999, and “Use of Metal Detectors in the Schools,” n.d.) will quickly pat down the suspect’s fully-clothed body. The pat down is the final step of a search and should be used only if necessary as the guidelines indicate. At any point during the search, if the object assumed to have set off the alarm is found, the search should end without proceeding through the remaining steps of the screening process.

When screening large groups, officials should follow similar procedures with only a few exceptions. For instance, because of the number of people being searched, the expectation for privacy could decrease, depending on the anticipated potential for violence: "the expectation of privacy that is reasonable should depend on the degree of harm" that the school is trying to "prevent or deter" (Song, 2003). Most likely, this type of surveillance would take place at the entrance to a school or in the school’s gymnasium rather than in a more private location like the principal’s office. All students would be searched, or if lines become too long, a random formula may be used to determine the selection of students to be screened. It should be noted, though, that there is a higher risk of discrimination when random selection is performed. There should in no way be any discriminating factors in the formula for choosing students to be screened, “for example gender, religion, race, etc.” (Shelby County School District, 2002). Rather, a more blanket formula should be used, such as every fourth person will be searched without exception, unless individualized suspicion overrides the rule. If a pat down becomes necessary, the suspect should be moved to a private location to continue the search. This stipulation is essential to promote privacy for the student.

Large-group screenings are not always effective or efficient, so they should be used sparingly and only if absolutely necessary as
deemed by school officials who have based their decision on excessive violent crime rates within the school district. One problem with large screenings is that they often take hours to complete, so “bottlenecks are common,” and oftentimes, students arrive to their first hour classes late if at all (Volokh & Snell, 1998). Schools try to solve that problem by using random selection of students on which to perform the search, but this is somewhat ineffective too because only a percentage of the students passing through the doors are being screened. When random searches are performed, as many as 8 out of 9 students walk through the door without being screened for weapons (Volokh & Snell, 1998). Another option is to have students arrive at the school at “staggering” times to “allow sufficient time for processing” (Schneider, 2001).

Still, for schools that have a reputation of routine violence, the statistics are convincing. Even with instances of large-group random screenings, the presence of metal detectors has proven to drastically reduce the number of violent crimes in the schools, and more and more schools are installing them to protect their students and staff. In Chicago, every public middle and high school has installed mounted metal detectors, and every public elementary school has at least two hand-held metal detectors (Hoffman, 2000). Many districts, however, do not have the immediate need for metal detectors in their schools. Very few elementary schools have any history of violence with weapons, so, appropriately, “fewer than one-half of 1 percent of elementary schools” had metal detectors at last count in 1996-97 (Hoffman, 2000). In 1998, only 15 percent of schools overall used metal detectors in any capacity—39 percent of urban schools used metal detectors; 10 percent of suburban schools used them; and only 6 percent of rural schools used them (National School Board Association qtd. in Volokh & Snell, 1998). “Perceptions of school violence as a nationwide problem do not justify the use of
metal detectors in local districts which have never had, and may never have, a problem with violence” (Ferraraccio, 1999). Once again, school officials must carefully assess their district’s need for surveillance and implement it appropriately.

Conclusion: How Can We Ultimately Conquer Violence in Our Schools?

“Prevention is a key factor in avoiding tragedies” (“U.S. Schools…,” 1997). Although “schools continue to be one of the most secure places for our children,” violence in schools is an issue that we must deal with swiftly through a combination of “‘hard’ responses such as metal detectors…[and] ‘soft’ responses that include more counseling, conflict resolution programs and better communications between school and home” (“School Safety,” 2003).

Some argue that “hard” responses, like metal detectors, are unnecessary. John Courtsunis’ (2001) solution is to “make everyone accountable in a more humanistic way and…work hard together for all involved, including the community at large.” Although this theory of an ethical utopia is appealing, it is not realistic. Prevention, or “early intervention,” programs definitely have their place in schools, but documentation on their independent success is very limited, whereas their use in conjunction with surveillance equipment is documented as highly successful. Don Weatherspoon, state assistant superintendent at Michigan, explains that “security is a larger issue than simple safety. That means having dispute resolution programs in schools as well as security cameras, school behavior rules as well as locker searches” (qtd. in Hoffman, 2000).

Some believe that “metal detectors are for beachcombers” (Courtsunis, 2001), while others believe that it is “better to be
safe than sorry” (Clark, 1999). Ultimately, it comes down to the school district though. “‘There is no one program, no silver bullet, so that you can get one program up and say, Here it is if you put this program in your school, you are going to resolve violence’….The ideal violence-prevention policy will likely be different for each school” (William Modzeleski, U.S. Department of Education, qtd. in Volokh & Snell, 1998).

References


Schneider, Tod. (Feb. 2001). Newer technologies for school


http://www.ojp.usdoj.gov/bjs/abstract/iscs02.htm


Project Creator Contact Information:
Kathy Davis, John Kelsey, Dia Langellier, Misty Mapes, and Jeff Rosendahl
Course - EPS 313
CTER program at UIUC
Course Instructor - Nicholas Burbules
Introduction

The National Education Association provides the following statistics:

* Every school day:
  
  - at least 100,000 students bring guns to school.
  
  - 160,000 students skip classes because they fear physical harm.
  
  - 40 students are hurt or killed by firearms.
  
  - 6,250 teachers are threatened with bodily injury.
  
  - 260 teachers are physically assaulted.
  
  - more Americans were killed by handguns between 1990 to 1992 (over 70,000) than were killed in Vietnam during the war (47,364). (Scrivner, n.d.)

At one time school safety was a minor focus for schools. President Ronald Reagan made school safety an issue in a 1984 radio address. (Stefkovich & Miller, 1999) Pointing out that violence in schools negatively affects learning and teaching, Reagan called on the country to begin solving discipline problems. (Reagan, 1984) School Safety became a more centralized focus of education after the many school shootings in the late 1990’s and early 2000’s. The response to these tragedies has ranged from proposals for new programs to teach children about guns to "character education" courses for students. (Tragedies spur action on school safety, 2000) Most schools have begun implementing several forms of surveillance to put a stop to the weapons and drugs that are infiltrating our schools. One method of surveillance that many schools have adopted to increase school safety and combat the distribution of drugs is the use of locker searches.
What are Locker Searches?

A locker search is simply the act of opening a locker and looking through its contents. Depending on the state, administration may choose to search one, several or all lockers. The search may begin when a drug dog indicates that there may be some contraband such as drugs in the locker, when a student reports concern of what another student may have in his locker, or when the administration calls for a random search.

A new locker has emerged on the market that will make locker searches easier. Smart lockers enable schools to follow student activity. (Smart lockers…, 2002) Smart lockers use swipe cards instead of padlocks and can be operated from a computer system located in a central office where one, or all lockers, can be opened. (Smart lockers…, 2002) The lockers can keep track of when a child is accessing his locker. Schools will even be able to track if a student is accessing his locker at a time when he should be in class and the number of times that he is using it in a day’s time. (Jonsson, 2002) “If a principal notices that a student is going in and out of his locker 18 times a day, that can raise suspicions,’ says Harry Popolow, senior project manager of Penco, a manufacturer of the smart lockers” (Jonsson, 2002).

Legality of Locker Searches

Many arguments have been made that locker searches are in violation of a child’s Fourth Amendment right. The Fourth Amendment states, “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” (Constitutional Ammendments…, n.d.) New Jersey v. T.L.O. was the first Supreme Court opinion to address the Fourth Amendment rights of students in public schools. (Stefkovich & Miller, 1999) In 1980, T.L.O. was found smoking in the restroom. She had been caught along with another girl. The one girl admitted her guilt and was suspended. T.L.O. denied smoking and the principal searched her purse and found a pack of cigarettes and rolling papers. He then proceeded to search the purse thoroughly and found some marijuana, a pipe, plastic bags, a fairly substantial amount of money, an index card containing a list of students who owed the respondent money, and two letters that implicated her in marijuana dealing. (New Jersey…, n.d.) The police and her parents were notified and she later admitted her guilt at the police station. Although this case defined the search of a child’s purse or bag and their Fourth Amendment right it did not go beyond the idea of a personal belonging’s search. The Supreme Court, in a New Jersey case decided in the 1990s, ruled that school officials don’t need a warrant or probable cause, but merely a "reasonable suspicion." (Gurr, 2002) Court rulings suggest
that students should have no expectation of privacy in school lockers when the school district both owns and controls the lockers and has a written policy describing this ownership. (Student Search, n.d.) In Zamora vs. Pomero, it was determined that the search of Zamora’s locker was not a violation of his Fourth Amendment right. (639…, n.d.) Even using dogs to search lockers and students is not an invasion of personal rights as established in Doe v. Renfrow. (The Use…, n.d.)

Rep. Kirk offered an amendment to H.R. 1350 on Wednesday, April 30, 2003; it was agreed to in the House by voice vote: The amendment expresses the sense of Congress that providing special needs students with a safe and drug-free learning environment is a laudable goal. (H.R. 1350 …, 2003) It makes reference to random locker searches conducted by school administrators as an effective way to assess the gravity of the drug situation at a particular school, as well as to indicate to students that the use of drugs on school property will not be tolerated. (H.R. 1350 …, 2003) In order for a locker to be searched at school, there must be reasonable suspicion. "Reasonable suspicion" means that the person initiating the search has a well-founded suspicion -- based on objective facts that can be articulated -- of either criminal activity or a violation of school rules. (Legal Guidelines …, n.d.) Reasonable suspicion is more than a mere hunch or supposition. (Legal Guidelines …, n.d.)

Many states have adopted legislation that allows for random searches of lockers. Suspicionless searches are not designed to catch offenders, but rather serve to prevent students from bringing or keeping dangerous weapons, drugs, alcohol, and other prohibited items on school grounds. (Moore & Milliken, 1999)

At what point does it become an invasion of students’ privacy? The NATIONAL ASSOCIATION OF ATTORNEYS GENERAL SCHOOL SEARCH REFERENCE GUIDE 1999 justified the right of schools to conduct random locker searches saying: “In Commonwealth v. Cass, 709 A.2d 350, 357 (Pa. 1998), the Supreme Court of Pennsylvania recently listed several reasons that justified the school official's ‘heightened concern’ as to drug activity in the school. These factors include:

- information received from unnamed students;
- observations from teachers of suspicious activity by the students, such as passing small packages amongst themselves in the hallways;
- increased use of the student assistance program for counseling students with drug problems;
- calls from concerned parents;
• observation of a growing number of students carrying pagers;

• students in possession of large amounts of money; and,

• increased use of pay phones by students. ”

Some of these factors seem a bit vague to start a random search of school lockers under the suspicion that there might be the distribution of a controlled substance or a weapon. Is it right to put all students to a search because there happens to be an increase usage of the pay phone? Has the administration asked any questions as to why there has been an increased use? It may be something as simple as a phone in contest that students are trying to win. Unless the administration chooses to ask more questions before conducting a random search, some students’ personal privacy will be infringed upon. A random locker search should only be conducted if there is an immediate threat to the student body. Sam Davis, dean of the University of Mississippi School of Law and an expert on constitutional issues surrounding school searches said, "The court over the last 15 to 20 years has really gone with preserving the government's interests over the individual's. There's really no question that students have less constitutional rights in a public school setting than they do outside." (Gurr, 2002) Wendy Wagenheim, ACLU legislative affairs director, said searches should only be conducted under reasonable suspicion. She went on to say, “An entire generation is being raised and trained in schools not to understand or appreciate the fundamental values of privacy and personal freedom from unreasonable searches and seizures that distinguish our society from a police state.” (Panel ponders…, 2000)

**Implementing Locker Searches**

A random locker inspection program does not involve direct law enforcement. (Moore & Milliken, 1999) A law enforcement agency may provide training for the administration but should not be present when random searches are conducted. All students and members of the school community, including parents and legal guardians, should be afforded notice in writing of the nature and purpose of the locker inspection program. (Moore & Milliken, 1999) Moore and Milliken recommend announcing the locker search procedure to the students in their homeroom or a school-wide assembly. They say “The whole point of the exercise (which is to deter drugs and weapons entering the school), after all, would be lost if the program were kept a secret.”

To prevent suspicions of bias and profiling, a “neutral plan” should be created. The plan should explain in precise detail how individual lockers or groups of lockers will be selected for inspection, taking into account that it is probably not feasible to open and inspect every locker in the school building every time that an inspection is
Drawbacks/Benefits

The main drawback to locker searches is the loss of privacy that students may feel. A locker is the only place in school that they can call their own. Many students decorate their lockers to reflect their own unique personalities. To have someone come in and search through their lockers and belongings to them is an invasion of privacy. There is also the issue of time. In order to do a school-wide search calls for the students to take time out of their classes to open their locker for the inspector. It is disruptive to the teacher and the class.

When drug-sniffing dogs come in to search the lockers, it often requires that the halls be clear of students. This too can cause problems. The search must be conducted while students are in class. Once they see or hear what is going on in the hallway, their attention will no longer be on the classroom material but on what is happening in the hall.

Even with all of the questions that surround the rights of students and their privacy when locker searches are conducted, there is still support for them to occur. In a poll of 600 people that was conducted in May of 1999 by Talmey-Drake Research & Strategy of Boulder for the Denver Rocky Mountain News and News4. Periodic locker searches were OK with 69 percent and 47 percent said they favor random searches of students. (Weber, 1999)

Though there are several drawbacks, the benefits far outweigh them. By conducting locker searches, the administrators lay the ground work for safer schools. It deters students from bringing contraband and weapons to school.

Recommendations

Each individual school knows which forms of surveillance best fit his/her needs. Locker searches are one way for schools to attempt to control the use of drugs and end violence in their school. When making the decision to implement locker searches in your school, several things must be considered.

Is conducting locker searches the best method of surveillance for your school? Does it meet the needs of your students and faculty? Is it physically conceivable to implement them in your buildings? How will your students and parents react to this intrusion of privacy? If after considering these questions you determine that locker searches are a method of surveillance you will be implementing in your school, there are two more things to think about.
A clear-cut policy on locker searches that all parents and students are aware of and have access to is a necessity. If a child is aware that a search of his locker can occur in his building, then the courts will stand behind the school provided the school is not infringing upon the students’ privacy as stated by the laws of that state. A model policy may be found at http://www.michigansafeschools.org/lockers.htm. In general, the more invasive the search, and the less reasonable cause, the more risky the search. (Womack, 2001)

The use of “Smart” lockers would be an excellent addition to the school. By having access to the number of times a student uses his locker in a day’s time, school officials can better attain reasonable suspicion. If that child is going to his locker 20 times in a day and only has six classes, it would raise some concerns. The next step would be to see what times he is using his locker. If the visits are at times when he should be in class, it again contributes to reasonable cause. This type of documentation will further support the school’s case in the search of that student’s locker. At $300 a locker, “Smart” lockers may not be the smartest choice for your school.

References


MODEL POLICY ON SEARCHES OF PUPILS’ LOCKERS AND LOCKER CONTENTS, (n.d.). Retrieved on...


Project Creator Contact Information:
Kathy Davis, John Kelsey, Dia Langellier, Misty Mapes, and Jeff Rosendahl
Course - EPS 313
CTER program at UIUC
Course Instructor - Nicholas Burbules
Surveillance in Schools: Safety vs. Personal Privacy

Internet Tracking

Introduction

As technology becomes more prevalent in schools and in the workplace, new problems come with it and some old ones are magnified. Slacking off, bullying, using company time for personal correspondence--these are all old problems that have been magnified with the addition of email and internet in the workplace. Spam, viruses, and bandwidth concerns are new ones. Many employers have chosen to deal with these problems by monitoring the incoming and outgoing email on their network as well as web browsing.

What is email monitoring?

With the advent of computers in the workplace has come the ability also to easily intercept and read other people's email without them being aware that it is being done. This is done one of several ways. It can be done through the use of software that will automatically save a copy of every email sent or received to a hidden location on your personal computer. A couple of examples of such software products are "Spectre Pro" and "eBlaster." Your email can also be intercepted by the Internet Service Provider (ISP). Every email you send goes first to the ISP and then is sent out to the Internet on its way to the recipient. Copies of email you have sent or received can easily be found on the server and read by someone with access to the server. Copies remain on the server for up to one year. Most people assume that once they delete an email, it is gone. Not true, as was discovered by Oliver North in the Iran-Contra investigations in 1987-1989. Deleted email messages between Oliver North and John Poindexter were retrieved in the investigation. Said Oliver North, "We all sincerely believed that when we send a PROFS message to another party and pressed the button 'delete' that it was gone forever. Wow, were we wrong." (Mikkkeee, n.d.) Those who use an email provider other than your ISP, such as Yahoo or Hotmail, leave themselves open to interception at this point as well. And finally, though there are many other points of interception, coworkers and system administrators or security officers at your place of work can also intercept your "private" email. Schools, as well as other employers, often act as your email provider and therefore have access to whatever you send or receive. In addition, as the email passes through the office network on its way to its destination, coworkers are capable of intercepting it as well. ("Top 10 Places Your Email Can Be Intercepted", 2000)

What is web monitoring?
Web monitoring ability has also been made widely available to employers, parents, and teachers. Web monitoring differs from simple web filtering in that it retains a record of web sites visited by a user, rather than simply blocking access to sites. Records of the sites visited are recorded in two different ways. Server based and client based software both record web browsing activities, but are installed either on the company's network, or on the individual computer. (Schulman, "Computer and Internet Surveillance...", 2002) The second method is most commonly used in the private sector by parents and spouses to monitor family members. Some examples of web monitoring software are SpectorPro, and SpyAgent. Software that makes use of a network to monitor and record web browsing is relatively inexpensive. It has even been recently employed by the U.S. Army who recently paid $1.8 million for a system that will watch over 200,000 workers, which works out to a cost of $9 per person. (Kirby, n.d.) Into this per person figure, the actual cost of monitoring web browsing must also be taken into account. Web monitoring software records browsing activity by either taking snapshots of the user's browser, by actively recording the entire browsing activity, or by creating a record of URLs with access times and dates.

Why monitor?

Internet monitoring is becoming more and more a common occurrence in the workplace. Between 1/3 and 1/2 of the US online workforce has its email and/or web surfing under continuous surveillance by employers. (Schulman, "Workplace Surveillance", 2002) A few of the primary reasons for schools or other places of employment, to use monitoring software is to prevent sexual harassment lawsuits, threatening viruses, bandwidth concerns and slacking off. (Schulman, "The Business & Technology...", n.d) Though these are valid issues, I would argue that constant monitoring is counter productive. It promotes an air of suspicion and hostility among the employees. Also, by tracking and storing details of employee's email and web browsing, the employer may inadvertently be storing potential evidence that could be used against him/her in future litigation. (Schulman, "One-Third or U.S...", 2001) Then there is the question of ethics and privacy. Should employers be looking at employees email? Should teachers look at students email? Is this like opening their mail? Is monitoring web browsing the same as standing behind the student in class?

The Ethical question--Is our right to privacy being usurped?

Most would use the analogy that the email message is like a telephone conversation. When you are talking on the phone, you only intend for the one person at the receiving end to hear your message. Similarly, you only intend for the receiver to read your email message. If wire tapping is an invasion of privacy, then, likewise, intercepting email messages ought to be as well. (Belanoff, 1999) The problem with this argument is that employers see the situation from a different angle. For them it is a property issue. The company is providing the computers and the network for...
your use; therefore, they have a right to ensure that they are not wrongfully using company resources. The fact that the sheer nature of the equipment makes this monitoring possible negates your expectation of privacy. (Belanoff, 1999) In addition, a phone conversation is auditory and needs to be secretly recorded to be saved and used by others, but an email is written conversation that passes through several portals on its way to its destination. It can be "discovered" by a number of persons along the way.

The main objections to internet monitoring seem to be that it invades our "right to privacy," or right to be left alone. Email users tend to assume that the same laws that protect their mail will protect their email and many employers take advantage of this by not making it clear to their employees that no such privacy exists. "People treat their emails like private letters, sealed and protected by law when in fact they are more like a postcard that anyone can read." (Meeks, n.d.) In addition, constant monitoring by some employers makes employees uneasy. Is it fair to monitor the email of every employee, even if no wrongdoing is suspected? Because there are so many points at which an email can be "discovered," the courts have generally found that there is no reasonable expectation of privacy. Perhaps a less invasive method would be to spot check, or only monitor the email of suspected abusers.

Some states do have laws governing the right to privacy of electronic communications modeled after the Electronic Communications Privacy Act of 1986 (ECPA). (Losey, n.d.) "The ECPA protects most electronic communications, including e-mail, from interception, attempted interception, disclosure, use, and unauthorized access." (Belanoff, 1999) There are exceptions that employees need to be aware of, however. For example, a company (or school district) that provides its own communications system may have the right to review and disclose its employees stored email. As I will discuss in the next section, one court case in particular reinforced the rights of employers to intercept email on the company email systems provided for employees.

Another exception to be aware of involves the consent of the sender and recipient. It is not necessary to have consent from both parties. If either gives consent to the monitoring, then email interception is permissible, according to ECPA. Consent could consist of simply signing a company email use policy. So even if you have not consented to email monitoring, if you send or receive an email to someone who has, your email could rightfully be intercepted.

The concern over email privacy is continually growing and evolving. As you will see below, when taken to court, sometimes the employer wins, sometimes the employee. Unfortunately, Congress has been unable to keep up with the rapid pace of evolving technology. The Privacy for Consumers and Workers Act (PCWN) was introduced in Congress in 1989-90 but has yet to pass and become law. If it were to pass, the PCWN would provide a national law to cover specifically the electronic monitoring of email and would require employers to provide their
employees with individualized notice before any actual monitoring took place. Again in 1999, a bill was introduced which would have required employers to give clear and conspicuous notice before monitoring. The Notice of Electronic Monitoring Act (NEMA) stalled in committee and has not been reintroduced. If employers laid out their electronic mail policies in a clear, concise manner, many problems of privacy could be avoided. After all, how can you expect employees to know how to use office email properly if they have never been told what is deemed appropriate? There remains the problem of email as a privacy or property issue, however. Employers often argue that the computer and network is provided for the employer and they have a right to ensure that company resources are not being misused. This has been argued a few times in court with the law usually siding with the employer.

**Court cases**

Though no definitive law has been passed yet, there have been several court cases regarding the interception of employee email. One such case is Smyth v. Pillsbury Company (1996) in which the federal district court in Philadelphia threw out an invasion of privacy claim against an employer. An employee was fired for statements he made to his supervisor via email. This employee had been told repeatedly that his (and all employees') email would not be monitored and would remain "privileged and confidential." Despite this, because the emails were discoverable at more than one point, the court ruled that "the employee had no reasonable expectation of privacy." (Schulman, "One-Third or U.S...", 2001)

In a similar case, Restuccia v. Burk Technology (1996), two former employees claimed that their employer invaded their privacy by intercepting their email communications in violation of a state wiretapping statute. They were terminated for the "excessive quantity" of their personal email usage. Once again, the court sided with the employers, saying that an employer's interest in storing computer information in backup files was a permissible wire "interception" allowed by the statute. Additionally, the court questioned whether the two employees had a reasonable expectation of privacy in their sending of email. (Belanoff, 1999)

Again in Bill McLaren, Jr. v. Microsoft Corp., the courts sided with the employer who used the "computer as company property" as a defense. Microsoft had provided Mr. McLaren with a personal computer and access to the company's email system. Mr. McLaren stored his personal email correspondence on the computer in a password protected folder. When accused of sexual harassment, Mr. McLaren told Microsoft that correspondence in this folder would exonerate him and he asked that they leave it alone. Microsoft subsequently discharged Mr. McLaren and obtained his email from this folder. The court found that "any e-mail messages stored in McLaren's personal folders were first transmitted over the network and were at some point accessible by a third-party. Given these circumstances, we cannot conclude that McLaren, even by creating a personal password, manifested -- and
Microsoft recognized -- a reasonable expectation of privacy in the contents of the e-mail messages such that Microsoft was precluded from reviewing the messages." (Samson, 2003)

The distinction between internal email and Internet email is an important one in the court system. In *Anderson Consulting L.L.P. v. UOP and Bickel & Brewer*, the employer was found not to be subject to the ECPA because the business provided its own internal email system and was not providing email access to the general public.

It would appear that the employee is at a definite disadvantage in the U.S. Courts. However, there have been some employee victories as well. In *McVeigh v. Cohen*, 983 F. Supp. 215 (1998), a sailor sued because he was dismissed from the Navy on the grounds that his email name brought his sexual orientation into question. The court found that the Navy had violated its "don't ask, don't tell" policy by obtaining information from America Online about the identity of the e-mail account holder. Additionally, in *Intel v. Hamidi*, the California Supreme Court ruled that Hamidi did not trespass on Intel's computer system when he sent six emails to Intel employees to inform them about what he considered to be Intel's abusive and discriminatory employment practices.

Because courts have ruled both ways in similar situations, employers could face legal problems if the company email policy is not carefully spelled out in a written policy. Districts considering email monitoring should consult with a lawyer about a written policy before proceeding.

**Benefits/Drawbacks**

For the school district, there are several benefits. The biggest advantage is probably the ability to eliminate spam and email viruses. Much time and money can be spent trying to purge the district's computers of viruses, and considering today's financial crisis in the public school system, monitoring seems like a wise choice. Bandwidth concerns are a high priority as well. Large attachments and spam both can clog a system and/or slow down the network. It is relatively inexpensive to monitor the system as opposed to upgrading the network.

A couple of other benefits that are seemingly more trivial is the prevention of bullying or sexual harassment and just general wasting of time. Cases of bullying or sexual harassment can be caught and dealt with early, thereby avoiding likely lawsuits. Additionally, the district would be able to prove that they knew of the problem and dealt with it in a timely manner. This has been an important issue in some email monitoring court cases. (see *Angela Daniels and Dimple Ballou v. WorldCom Corp.*) This could be a drawback as well, if the district did not take prompt action against an employee guilty of bullying or sexual harassment.

What about the employees' privacy though? Teachers will not want to lose their privacy by having their incoming
and outgoing email messages monitored. This is assuredly a drawback. A school district will not want to risk creating a hostile work environment by leaving the impression that they are suspicious of everybody. Constant monitoring of the entire internet system is probably not a good idea then. Also, there is the risk that lawsuits could be brought against the district, claiming invasion of privacy or that the district did little to stop harassment. A carefully crafted internet policy is a necessity to insuring that no expectation of privacy is given. As for the harassment issue, this is something to weigh very carefully. Is the district better off monitoring for this kind of thing, or should they worry about having proof of not handling a harassment issue quickly enough?

**Is monitoring students different than employees?**

As more and more schools begin to incorporate technology into their curriculums, they are faced with the decision of whether to allow students to use email at school or not. Some have taken the easy route and have forbidden student email accounts. Others, seeing the educational value of email for class projects, have decided to allow it but to monitor it for the students’ safety. Again, districts face the privacy issue as a drawback. However, the advantages are not always the same as for the teachers. While monitoring students internet activities are still important for reasons of viruses and bandwidth issues, the bigger issue is protecting students, both from outside influences and from bullying by other students. Although students may consider monitoring their email an intrusion on their privacy, is it any different than intercepting a note passed in class between two students? This has been done for centuries without cries of invasion of privacy. As long as students have read and signed an Acceptable Use Policy (AUP) explaining the rules, they should not expect their emails or web browsing at school to be private. Schools must consider the fact that some parents consider the Internet to be a danger and expect their children to be protected.

The method of monitoring for students is usually different as well. Depending on the age of the students, teachers can set up one email account per class, thus making it easier to monitor the email coming and going or can set up a student email account through a system such as ePals or eChalk. These email programs allow the monitor to set the level of controls to an appropriate level for the age level of the students. This ranges from previewing all incoming and outgoing messages to flagging a message that contains certain words to be previewed before reaching its destination.

There is seemingly a conflict between protection of students and allowing the students to explore as part of the learning process. If we monitor students' correspondence and browsing activities, they may be prevented from gaining access to some valuable information. Should this be sacrificed in the name of safety? Where do we draw the line between protecting children and allowing them to explore and learn? ePals and eChalk are two examples of software that try to deal with this issue. Because the controls can be set at varying levels, monitoring can be much
more stringent at the grade school level than at the high school level.

**Recommendation to Schools**

Without some controls in place, schools could face slower networks, a glut of spam, viruses, and possible misuse of email for harassment, etc. Before putting anything into place however, it is important that teachers have a clear and concise email use policy to read and sign and students have an AUP in place as well. This helps to eliminate the expectation of privacy that many wrongfully assume they have when it comes to email. It also lays out exactly what is expected of students and teachers when it comes to email use. It is much easier to follow the rules when everyone knows exactly what they are. (Spykerman, 2003) Some suggestions with regard to email monitoring:

1. "A copy of the policy should be signed by each employee before he or she is allowed Internet and/or e-mail access. The policy should include a clear statement that derogatory, obscene, defamatory and/or harassing communications are prohibited and will lead to disciplinary action up to and including termination."

2. "Employers can purchase the same software sold to parents who wish to block children's access to sex-related Internet sites. Some Web browsers even have settings built in that will permit the employer to do this. (The employer's failure to take advantage of such a feature can give employees a colorable argument about the employer's acquiescence to unrestricted use)."

3. "Employers can purchase computer programs which track access to the Internet. Although these programs do not block access to sex-related material, they create a record of activity by employees on the Internet. If you implement such a program, employees should be advised, in order to limit their expectation of privacy. Also, a warning that 'we know who you are and where you have been,' may persuade some employees to avoid accessing sex-related Internet sites. Do these programs work in a way that amounts to 'interception' or 'access' to stored information for purposes of the ECPA or similar state statutes? No one knows yet."

4. "Employers can state that misuse of e-mail and Internet are violations of the company harassment/discrimination policy. Specifically, employers should institute and enforce uniformly policies that prohibit use of company equipment to access, possess, or forward offending material, regardless of sexual content."

5. "Employers should engage in consensual monitoring of e-mail messages on a regular basis. Proper auditing and monitoring of e-mail files may assist employers in identifying problem areas before legal action is started and they are forced to produce damaging material. Employers should develop an auditing program that will be effective and efficient. An audit of all company e-mail is too burdensome. Rather, an employer should use more focused methods. This may include random monitoring of e-mail files and checking the hard copy printed off the terminal to determine compliance with corporate record retention policies. Some employers may choose to have all employees with computer access sign an annual statement that they have followed the
corporate policy with respect to e-mail use. Some employers even install programs that bring up a consent statement every time the computer is started, and require the employee to press an "I agree" button to proceed." (Belanoff, 1999)

Sample email use policies can be found in the appendix of E-mail: Property Rights vs. Privacy Rights in the Workplace (with Model Consent Forms and Communications Policy). AUP's should also contain specific references to what is deemed appropriate email usage. Schools should spell out the things that are not appropriate, such as sex-related material, offensive, obscene or harassing material, hate/violence related material, foul language, etc.; as well as the consequences of violating the AUP. It should be noted that privacy is not a reasonable expectation, and students should be told exactly how the email system is monitored. A signature should be required annually, without which email access will be denied.

For the sake of morale, the monitoring that takes place should be in the form of spot checks when there is reason for suspicion. Simply having an email use policy in place that says teachers and students will be monitored will promote proper email habits for the most part. (Mikkekee, n.d.) For student email accounts, a suggested way to go is to use a system such as ePals that can be set at different levels according to the age levels of the students. This will route all student email through an assigned "monitor." Another suggestion for both students and teachers is to employ a flash screen that reminds them that their emails are being monitored each time they use the system. It's not enough to have them sign an email use policy annually; they should be reminded often to use the system properly.

In conclusion, should a district decide that email monitoring is necessary, it is important to have a written Email Use Policy for teachers and an Acceptable Use Policy for students in place before doing any monitoring. Failure to do this leaves the district open to possible lawsuits. Whether a district chooses to monitor or not, this Email Use Policy/ AUP will help guide employees/students in using email appropriately. Despite the conflicts over privacy issues and restrictions on learning, some monitoring is necessary to ensure that acceptable email use is being carried out. Simply stating what is expected in an email use policy is insufficient if there is no way to check to see if the rules are being followed so that they can be enforced.

References


Meeks, Brock N. (n.d.) Surveillance at Work "Big Boss is Watching". Retrieved 7/19/03 from: http://www.mediacritica.net/courses/335/privacy.html


Privacy for Consumers and Workers Act. (n.d.) Retrieved 7/20/03 from: http://www.eff.org/Privacy/Workplace/s984_consumer_workplace_priv.bill


Project Creator Contact Information:
Kathy Davis, John Kelsey, Dia Langellier, Misty Mapes, and Jeff Rosendahl

Course - EPS 313
CTER program at UIUC

Course Instructor - Nicholas Burbules