

I. Student Use and Misuse of Technology.

A. School Discipline – Websites, E-mails, and Cyberbullying.

1. *J.S. v Bethlehem Area Sch. Dist.*, 807 A.2d 847 (Pa. 2002).

Issue: Whether a school district may discipline a student, consistent with the First Amendment, for creating a website at home and posting it on the Internet, when it contained derogatory, profane, offensive, and threatening statements directed toward a teacher and his principal who saw the site at school?

Facts: An eighth grade student created a website entitled “Teacher Sux” on his home computer, on his own time, and posted it on the Internet. The website was not sponsored by the school district. It consisted of web pages that made derogatory, profane, offensive, and threatening comments in the form of written words, pictures, animation, and sound clips. For example, it included a picture of his teacher with a severed head dripping with blood and a solicitation for funds to cover the cost of a hit man. One web page indicated that the principal engaged in sexual relations with a principal from another school. When the principal and teacher viewed the site at school, each took the threats seriously. The student was expelled from school and, subsequently, sued the school claiming First Amendment speech rights.

Holding: The Supreme Court of Pennsylvania affirmed the lower court ruling in favor of the school district. First, the court concluded that the student’s speech was not a “true threat,” an exception to the right of free speech, and cited the fact that the district allowed the student to attend class and extracurricular activities during an investigation of the incident. Second, however, the court concluded that although the website was created off-campus, it was accessed and viewed at school. In upholding the student’s expulsion the court reasoned that student free speech rights must be balanced with the school officials’ need to maintain order and to discipline when necessary to assure a safe school environment that is conducive to learning.

2. *Coy v. Bd. of Educ.*, 205 F. Supp. 2d 791 (N.D. Ohio 2002).

Issue: Whether a school district may expel a student consistent with the First Amendment when he creates a website from home and posts it on the internet, when it contained crude, profane, and sexually suggestive content?

Facts: A student was expelled for 80 days after he created a website from his home computer which was intended to describe the exploits of the

student and his friends; there was also a section entitled “losers” which referred to another group of students, and had a few insulting sentences about the other group of students. The whole webpage was created at the student’s home; the student, on at least one occasion, accessed the website from school.

Holding: The court found that the website was crude, profane, and sexually suggestive, however, it was not obscene. The court found that if the school district expelled him because of the content of the website, then it was in violation of the student’s First Amendment rights. However, if the school disciplined the student because his accessing the website from school caused substantial disruption, then discipline might be appropriate. The court ultimately determined that there were too many issues of fact left to determine.

3. ***Layshock v. Hermitage Sch. Dist.*, 496 F. Supp. 2d 587 (W.D.Pa. 2007).**

Issue: Whether a school district may suspend a student who has created an off-campus myspace.com parody profile of his principal?

Facts: A high school senior created a parody profile of his principal and received a ten-day suspension. The district punished him for causing disruptions of the normal school process; harassing a school administrator; engaging in gross misbehavior; using obscene, vulgar, and profane language; violating the school’s computer policy; and using school pictures without authorization. The student was also placed in an alternative curriculum program and was forbidden from attending school-sponsored events and graduation. The student challenged his punishment by asserting that the school violated his First Amendment right to free speech.

Holding: The court stated that schools have much more limited authority over off-campus speech than speech that occurs on campus. The school also needs to establish a sufficient nexus between the offending speech and a substantial disruption of the operation of the school. The school did not establish such a nexus; the school did not establish whether the students’ discussions were about the actual profile or were about the school’s reaction to the profile. Lastly, the court noted that any actual disruption was minimal because no classes were cancelled and there was no widespread disorder, violence, or disciplinary action.

4. ***Killion v. Franklin Reg’l Sch. Dist.*, 136 F. Supp. 2d 446 (W. D. Pa. 2001).**

Issue: Whether a school district may discipline a student consistent with the First Amendment when he sends e-mails from home to friends’ homes

that contain offensive and obscene language about the school's athletic director?

Facts: A student created a "Top Ten" list about the school's athletic director, including statements about the director's physical appearance and genitalia, while at home after school hours. The student e-mailed the list from his home computer to friends at their homes. He did not print or copy the list to bring on school premises because he had been warned about such behavior after copying and distributing similar lists in the past. However, an unknown person brought the student's list to campus and distributed it. The student admitted creating the list and was suspended for the offensive remarks about a school official in the list found on school grounds. The student sued the school claiming First Amendment speech rights.

Holding: The court ruled in favor of the student, finding the district violated the First Amendment because it failed to satisfy the "substantial disruption test." There was no evidence the teachers were incapable of teaching or controlling their classes because of the list, which was, in fact, on the campus for several days before the administration became aware of its existence, and the administration waited one week before taking any action. Furthermore, even though the list contained lewd and obscene language, which might be punishable in the school context, there was no evidence the student was responsible for bringing the list to school.

5. ***Emmett v. Kent Sch. Dist. No. 415, 92 F. Supp. 2d 1088 (W.D. Wash. 2000).***

Issue: Whether the student's First Amendment rights were violated when the school district expelled him for intimidation, harassment, disruption to the educational process, and violation of school copyright rules because he posted a web page on the Internet from his home that consisted of mock obituaries?

Facts: A student created a web page from his home without using school resources or time that consisted of tongue-in-cheek, mock "obituaries" of two friends. A creative writing class in which students were assigned to write their own obituary inspired the page. The student also allowed visitors to the website to vote on who would "die" next, that is, who would be the subject of the next mock obituary. The website became a source of discussion at the school and on the evening news, it was characterized as featuring a "hit list" of people to be killed. The website, however, did not use the words "hit list" anywhere on the site. The school initially expelled the student, but modified it to a five-day short term suspension. The suspension included a prohibition on participation in school sports,

including basketball practice and the team playoffs. The student sued the school seeking an injunction against the short-term suspension.

Holding: The court held for the student, finding that missing four additional days of school and sporting events would cause him irreparable injury when balanced against the hardships presented by the school district. The school district failed to show that any student actually felt threatened by the website, or that the student had any intent to intimidate or threaten anyone. Although the court sympathized with the school's concern that websites can be an early indication of a student's violent inclinations and can spread those beliefs quickly to like-minded or susceptible people, it rejected the school's claims that the suspension was necessary. The school's case was based on a lack of evidence, and the undifferentiated fear of possible disturbances or embarrassment to school officials was insufficient to support their claim.

6. ***Doninger v. Niehoff*, 527 F.3d 41 (2d Cir. 2008).**

Issue: Whether a student's rights to free speech under the First Amendment were violated when she was prohibited from running for a class office after she posted a vulgar and misleading message on a publicly accessible blog?

Facts: After learning that a band event was going to be postponed, the student e-mailed members of the community regarding the rescheduling of a band contest. After receiving numerous responses, the principal requested the student to send a corrective e-mail. Instead, the student posted a blog while off-campus, which contained vulgar language. The blog erroneously asserted that the contest had been cancelled, and urged readers to contact the school. Concluding that the student's conduct failed to display the civility and good citizenship expected of class officers, the principal prohibited the student from running for class office.

Holding: The Court of Appeals for the Second Circuit agreed with the district court in saying that her rights under the First Amendment were not violated. We recognized that off-campus conduct can create a foreseeable risk of substantial disruption within a school; in such circumstances, its off-campus character does not necessarily insulate the student from school discipline. In this case, the student created this blog for the purpose of it coming on campus. This case demonstrates that courts are less hesitant to discipline students for inappropriate use of technology and are more apt to consider the cumulative effects of behavior that is sufficiently disruptive.

7. State Laws.

a. Statutory Authority to Suspend Students (Wis. Stat. § 120.13(1)(b)(2)d).

Permits suspension for: “conduct while not at school or while not under the supervision of a school authority that endangers the property, health or safety of others at school or under the supervision of a school authority or endangers the property, health or safety of any employee or school board member of the school district in which the pupil is enrolled.”

b. Statutory Authority to Expel Students (Wis. Stat. § 120.13(1)(c)1).

Permits expulsion when the board finds that a student: “while not at school or while not under the supervision of a school authority engaged in conduct which endangered the property, health or safety of others at school or under the supervision of a school authority or endangered the property, health or safety of any employee or school board member of the school district in which the pupil is enrolled, and is satisfied that the interest of the school demands the pupil’s expulsion. In this subdivision, conduct that endangers a person or property includes making a threat to the health or safety of a person or making a threat to damage property.”

c. Electronic Communication Devices Prohibited (Wis. Stat. § 118.258).

Each school board may adopt rules prohibiting students from using or possessing an electronic communication device while on the premises of a public school and provide them to each student annually.

8. First Amendment Rights.

School districts may punish student conduct that materially and substantially interferes with the requirements of appropriate discipline in the operation of school. Threats of violence, if true threats, are not protected by the First Amendment. A student who maintains a website, blog, or other forum cannot be punished for comments or posts written by others, when the student was merely the provider of the forum.

B. Search and Seizure of Electronic Communications Devices.

The search and seizure of communications devices when officials suspect a device is being used inappropriately is an emerging legal issue. For example, school district officials may receive information that a student has secretly taken photographs of other students in locker rooms. If so, school district officials may decide to seize the cellular phones and search their contents to determine the validity of the allegations.

1. *Klump v. Nazareth Area School District*, 425 F. Supp. 2d 622 (E.D.Pa. 2006).

This case serves as a warning to school administrators regarding their investigative techniques that may include a review of their contents of such devices. In *Klump*, school officials confiscated a high school student's cellular phone because he displayed it during school hours in violation of school policy. While the school officials had the telephone, they accessed the student's phone directory and started making calls with the phone. They called nine other high school students listed in the directory to determine whether they too were violating the school's cellular telephone policy. The officials also accessed the student's voicemail and text messages and conducted an instant message conversation with the student's brother without identifying themselves as being anyone besides the student. Based on these actions by the school officials, the student and his parents filed a ten-count complaint in federal district court against the school district, superintendent, assistant principal, and teacher alleging several federal and state crimes.

Included in the complaint, the student alleged that the school officials violated his Fourth Amendment right to be free from unreasonable searches and seizures. The court denied the official's request for immunity.

The federal court concluded that the school official's were justified in seizing the phone because the student had displayed it in school, violating the school's policy prohibiting the use or display of cellular phones during school hours. However, the court decided that the school officials failed to meet the reasonableness standard that is required when they accessed the telephone directory, voicemail, and text messages, and called other students. According to the court, the school officials did not have any basis for initiating a search because they had no reason to suspect that such a search would reveal that the student himself was violating another school policy. Instead, the court concluded that the school officials were unlawfully conducting a search to find evidence of other students' misconduct. Before conducting any search of non-contraband items,

school district officials must make sure that they have reasonable grounds to believe that such a search will turn up evidence that the student has violated or is violating either the law or the rules of the school.

The court found that the plaintiff student could bring a claim under the Wiretap Act for unlawfully accessing the plaintiff's stored voicemail and text messages.

C. Cell Phone Jamming Devices.

1. Federal Law. Communications Act of 1934 (47 U.S.C. § 333).

A cell phone jammer operates by emitting a frequency that collides and then cancel the cell phone signal out, thus preventing cell phone communication. In 2005, the Federal Communications Commission issued a public notice declaring the sale and use of transmitters "designed to prevent, jam or interfere with the operation of cellular or personal communications service ... unlawful." (FCC Public Notice DA-05-1776); 47 U.S.C. § 302a(b); FCC Rules Sec. 2.803(a). According to the FCC, jammers fall under the Communications Act of 1934 prohibiting any person to "willfully or maliciously interfere with the radio communications of any station licensed or authorized under the Act or operated by the U.S. Government." 47 U.S.C. § 333. The stated penalties for parties in violation include monetary forfeitures up to \$11,000 a day for each violation and the possibility of further criminal prosecution.

Mt. Spokane High School in Spokane, Washington tested the use of a cell phone jammer in order to block students from sending text messages and making phone calls. The jamming device was turned on during class time and turned off during passing periods and lunch hours. Days after the testing, the school district decided to end the program and returned the jammer to the seller. District Administrators cited FCC regulations as well as concerns over emergency situations as reasons for not implementing the technology.

School officials at the Penn Hills School District, in suburban Pittsburgh, Pennsylvania, voted whether to consider buying equipment which would prevent students from telling each other where to meet for fights or where security guards may be. Upon learning of the FCC regulations, the superintendent announced the district would be looking into other options.

In Port Hardy Secondary School, British Columbia, a high school principal became so frustrated that a cell phone ban in his school was not effective that he bought a cell phone jammer from a dealer in China. The device was installed in the school library. After students and parents

voiced concerns that their rights were being violated, the principal removed the device.

The St. Ansgar School Board in Northern Iowa passed a motion to spend up to \$5,000 to jam cell phones in their schools. Policy was already in place where any cell phone being used at school would be confiscated and then returned to the student after the school day. After a second incident, parents had to come to the school and pick up the phones. The plan was to have the jammer in place to block signals except in emergency situations. However, after learning of the FCC rules, the school district dropped the plan.

D. Criminal Conduct.

1. *Boucher v. School Bd. of the Sch. Dist. of Greenfield*, 134 F.3d 821 (7th Cir. 1998).

Issue: Whether a student violated the state criminal computer law and school policies regarding student use of school district computers when he distributed an article at school entitled, “So You Want To Be A Hacker?”

Facts: The student wrote an article entitled “So You Want to be a Hacker” outside of school, published it in an underground, unofficial newspaper, and then brought it to school and distributed it in bathrooms, lockers, and in the cafeteria of Greenfield High School. The article described how to enter the computer’s setup utility, see a list of every file on the computer, with student and teacher login names, and attempt to find the password for entering the files. The Board concluded that the article provided instruction to unauthorized persons on how to access the school district computer programs and disclosed restricted access information to the school district’s computers. The student was expelled for violating the Board policy on the use of the school district computers, network and the Internet and general school rules for behavior and communications by its students with its computers. The student sued the school district for violating his First Amendment right to speak freely on the subject of computer use and hacking.

Holding: The Seventh Circuit Court of Appeals found in favor of the school district, reversing the federal district court ruling. The court reasoned that “[t]he Supreme Court has repeatedly emphasized the need for affirming the comprehensive authority of . . . school officials, consistent with fundamental constitutional safeguards, to prescribe and control conduct in the schools.” The court found that the school district faced substantial harm when confronted by the self-proclaimed, student hacker if the district court injunction was enforced against their disciplinary efforts. The court concluded that the article, distributed on

campus with the student's knowledge, purported to be a blueprint for the invasion of the school's computer system, as well as encouragement to do just that—a call to action detrimental to the tangible interests of the school and endangering school property.

2. ***Spielmann v. Hayes*, 2000 OK CIV APP 27, P.3d 711.**

Issue: Whether the court could enforce a protective order obtained by a teacher against a student when the student left a voice mail threat on the teacher's school voice mail system directed at the teacher's husband?

Facts: A message was left on the 7th grade science teacher's school voice mail that threatened to kill her husband if she disciplined any students. When the teacher retrieved the message, she contacted the principal and two other administrators. The teacher recognized the voice as one of her students. The student was expelled from school. The teacher filed a petition for a protective order against the student as a victim of harassment, defined by the Oklahoma statutes under the Protection From Domestic Abuse Act. The trial court ordered the student not to abuse, injure, visit, threaten, or harass the teacher. The student challenged the order.

Holding: The court affirmed the order. Even though the threat was directed at the teacher's husband, the student had engaged in a course of conduct of choosing to leave a voice mail message containing an articulated death threat, alarming the teacher, causing her substantial emotional distress, and serving no other legitimate purpose than to require the teacher to alter her course of conduct by not sending any student to the office in order to avoid the death of her husband.

3. **State Law.**

a. **Computer Crimes Act (Wis. Stat. § 943.70(2))**

Willful, knowing, and unauthorized offenses against computer data and programs, including copying, modifying, destroying, accessing, or disclosing restricted access codes to unauthorized persons, of data, computer programs or supporting documentation is a crime.

b. **Unlawful Use of Computerized Communication Systems (Wis. Stat. § 947.0125).**

Intentional conduct consisting of frightening, intimidating, threatening, abusive, or harassing messages sent to a person on an electronic mail or other computerized communication system with

the threat to inflict injury or physical harm to any person or property is a crime.

c. Harassment (Wis. Stat. § 947.013).

Harassment means a pattern of conduct or repeatedly committing acts representing a credible threat which harass or intimidate another person.

- i. Harassment includes striking, shoving, kicking or otherwise subjecting another person to physical contact or attempting or threatening to do the same.
- ii. The statute refers to actions against a “person,” which has been interpreted by case law to include municipalities. A school district, therefore, is an entity entitled to obtain injunctions and may do so when there is a relationship between the harassing conduct and the school.
- iii. Case law confirms that the statute does not violate protected speech, rather, it is directed at oppressing repetitive behavior which invades another’s privacy interests in an intolerable manner.

II. Employee Use and Misuse of Technology.

A. Secretly Taping a Meeting with a Supervisor.

1. *Claridge Products & Equip., Inc.*, 94 Lab. Arb. (BNA) 1083 (1990).

Employee placed a tape recorder in the department supervisors’ office, where he hid a tape recorder on the top shelf when the office was empty, switched it on to “recording” position and claimed that he left it there for safekeeping. When the employer discovered the recorder, the employee was terminated. After concluding that the employee placed the tape recorder in the supervisors’ office for the explicit purpose of taping their conversations in order to benefit himself, the arbitrator upheld the termination as being for just cause.

2. *Moen v. Town of Fairfield*, 713 A.2d 321 (Me. 1998).

Plaintiff Moen, a police officer and also the Union Steward, secretly taped his conversations with the Chief of Police because the officer distrusted the Chief and wanted to preserve an accurate record of their conversations for future grievance proceedings and other possible legal actions. Moen played the recordings for various others, including both officers and

citizens outside the department. Also, Moen encouraged others to secretly record their meetings with the Chief of Police. Moen argued that his action in taping the meetings was protected by the First Amendment to the U.S. Constitution. The court disagreed.

3. ***Atwood Mobile Prods.* 326 N.L.R.B. 1196 (1998).**

An employee, Williams, taped her investigatory interviews with her supervisor, Nitz, and played it for other employees. When Nitz learned that Williams had taped their meeting, he asked her for the tape and she admitted to taping the meetings, but refused to turn over the tape to him. As a result, he terminated her because she had taped the meetings. She said her attorney had advised her to record the conversations. The employer had a policy that required employees to keep disciplinary matters confidential. Nitz believed Williams' conduct in taping the meetings and playing the tapes for others violated this policy.

The Board noted that there was no rule against the surreptitious tape recording of conversations with management. Given this, as well as other evidence establishing anti-union animus, the Board concluded that Williams' discharge was an unfair labor practice in violation of the NLRA.

B. Government Regulation and Civil Prohibition of Employee Computer Usage.

1. ***Urofsky v. Gilmore*, 216 F.3d 401 (4th Cir.), cert. denied, 531 U.S. 1070 (2001).**

Issue: Whether a state regulation prohibiting state employees' access to sexually explicit material on state computers is consistent with the First Amendment and their right to academic freedom?

Facts: Six professors employed by various public colleges and universities brought suit against the state of Virginia, challenging a law restricting state employees from accessing sexually explicit material on computers that are owned or leased by the state without permission.

Holding: The court held that regulation of state employees' access to sexually explicit material, in their capacity as employees, on state computers is consistent with the First Amendment. The court cited judicial precedence for the proposition that the state, as an employer, possesses greater authority to restrict the speech of its employees than it has as a sovereign to restrict the speech of ordinary citizens. The threshold question is whether the state law regulates the speech of state employees on matters of public concern in their capacity as citizens. Additionally, the court found no judicial support for a right to academic

freedom above the protections afforded to all public employees against dismissal for the exercise of First Amendment rights.

2. ***Strauss v. Microsoft Corp.*, 814 F. Supp. 1186 (S.D.N.Y 1993).**

Issue: Whether e-mail messages could be used to support a claim of sexual harassment and discrimination?

Facts: A female employee at Microsoft received at least four separate e-mail messages from a supervisor that “contained sexual innuendo,” such as referring to another woman in the office as the “Spandex Queen.” She sued Microsoft for gender discrimination, relying, in part, on the e-mail messages as evidence. The supervisor had put the e-mail messages into personal folders on his work computer with his own password. The company policy allowed employees to do that, and the supervisor thought the messages were, therefore, secure. However, during the investigation of the supervisor, the company “broke into” the personal files and retrieved the messages. The defendant challenged the use of the e-mail messages as evidence at the trial.

Holding: The court ruled that the e-mail messages were admissible as evidence at the trial.

3. ***Greenslade v. Chicago Sun-Times, Inc.*, 112 F.3d 853 (7th Cir. 1997).**

Issue: Whether the frequency with which an employee sent unwanted e-mail messages to a coworker contributed to a finding of harassment?

Facts: Editors at the newspaper frequently communicated with coworkers about both business and personal matters via an electronic mail (e-mail) system. Greenslade was an editor who had created an inventory of multi-colored “form” e-mail messages for business and personal reasons which could be sent quickly to one or more coworkers. Included among his “form e-mails” was one in which he offered rides home to coworkers who had not driven to work. Shortly after a female coworker, Wagner, began work at the paper, Greenslade began offering her rides home. She initially accepted some of these offers. However, over a period of time, the quantity and content of e-mail messages Greenslade sent Wagner began to concern her. She was receiving more personal e-mails from Greenslade than from anyone else at the newspaper. Greenslade was removed from his position and transferred to another position with the company. He challenged the transfer.

Holding: The court ruled in favor of the company, finding that Greenslade engaged in unwanted, questionable behavior, in part, because of the *excessive number* of personalized e-mails he had sent Wagner.

4. ***Blakey v. Continental Airlines, Inc.*, 164 N.J. 38 (N.J. 2000).**

Issue: Whether an employer, who has notice that co-employees are engaging in retaliatory harassment directed at another co-employee by using a computer bulletin board created by the company, has a duty to remedy that harassment?

Facts: A female pilot filed systematic complaints with representatives of Continental Airlines, complaining of sexual harassment and hostile work environment based on conduct directed at her by male co-employees in the plane's cockpit and other work areas. The conduct included displays of pornographic photographs and vulgar gender-based comments. When Continental failed to remedy the hostile work environment, the pilot filed a charge of sexual discrimination and retaliation in violation of Title VII of the Civil Rights Act.

In the midst of the federal litigation, fellow pilots continued to publish a series of harassing gender-based messages on the pilots' on-line computer bulletin board. The bulletin board was accessed through the company's Internet provider, where a forum for Continental pilots and crew members was available. Individual postings stated that the female pilot's allegations were false, that the lawsuit was motivated by greed and selfishness, that she had poor piloting and interpersonal skills, and that female pilots were looking for favorable treatment. One example was a posting stating, "I also heard you crashed your floatplane . . .," which the female pilot called false and defamatory.

Holding: The state supreme court held that the electronic bulletin board should be regarded as part of the workplace, and that the postings could have constituted a hostile work environment. Furthermore, "when the employer knows or has reason to know that such harassment is part of a pattern of harassment that is taking place in the workplace and in settings that are related to the workplace," employers have a duty to take effective measures to stop co-employee harassment.

C. **Federal Legislation.**

1. **Protection of Children Against Sexual Exploitation (18 U.S.C. § 2252).**

A crime is committed when any person knowingly transports or receives in interstate commerce, including by computer or mail, any visual depiction, if (a) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and (b) such visual depiction is of such conduct.

D. State Legislation.

1. Possession of child pornography (Wis. Stat. § 948.12).

Whoever knowingly possesses any undeveloped film, photographic negative, photograph . . . pictorial reproduction or audio recording of a child engaged in sexually explicit conduct is guilty of a felony.

III. Employer Use and Misuse of Technology.

A. Privacy Rights: Video Surveillance, E-mail and Voice Mail.

1. *Vega-Rodriguez v. Puerto Rico Telephone Co.*, 110 F.3d 174 (1st Cir. 1997).

Issue: Whether the company's continuous video surveillance of the work area violated privacy rights and Constitutional protections?

Facts: Puerto Rico Telephone Company is a quasi-public corporation. Employees sued the company challenging videotaping of their workplace as an invasion of their privacy and a violation of the Fourth Amendment Rights. The work space inside the company's Executive Communications Center consists of a large L-shaped area containing computers, monitors, furniture, etc. The work space is completely open and no individual employee has an assigned office, cubicle, work station, or desk. Three video cameras survey the work space, and a fourth tracks all traffic passing through the main entrance. Cameras do not cover the employee rest area. The surveillance is exclusively visual; the cameras have no microphones or other immediate eavesdropping capability and operate all day, every day. No one is allowed to view the monitor or completed tapes without the general manager's express permission.

Holding: The court upheld the use of video surveillance of employee work space. First, the court reasoned that business premises invite lesser privacy expectations than do residences. Second, the court found that the physical layout of the work area belied any expectation of privacy. Third, the court found that the nature of the intrusion, monitoring space that is in plain view within an open area, strengthened the employer's legitimate interests. Finally, the court noted that employer policies and regulations can provide a warning to employees that certain areas are subject to employer intrusions, reducing their expectations of privacy. The court concluded that unconcealed video cameras not equipped with microphones, which record only what the human eye could observe, did not violate the employee's privacy or constitutional rights.

2. ***Cramer v. Consolidated Freightways Corp.*, 209 F.3d 1122 (9th Cir. 2000), cert. denied, 122 S.Ct. 806 (2002).**

Issue: Whether privacy rights were violated when the company surreptitiously videotaped restrooms through two-way mirrors when the collective bargaining agreement with the union included the use of video cameras?

Facts: Several truck drivers brought a class action suit against a California trucking terminal alleging invasion of privacy and infliction of emotional distress when it was discovered that the company was videotaping in the restrooms. California law prohibits placing cameras or two-way mirrors in restrooms. The case became known as the “potty privacy” controversy. The company said it installed the cameras to try to stop the sale and use of drugs in the restrooms and aimed the cameras away from urinals and toilets. It claimed that the Union had agreed to video surveillance as part of an employment contract and, therefore, could not expect privacy even in the lavatory.

Holding: The court dismissed the invasion of privacy and infliction of emotional distress claims because the collective bargaining agreement allowed both video surveillance and drug testing. The court agreed with the trucking company that the privacy claim could not be determined without interpretation and application of the collective bargaining agreement because the employees alleged that they reasonably expected to be free from video surveillance. The claims, therefore, fell within the preemptive reach of the Labor Management Relations Act, 29 U.S.C. § 185. One judge dissented, however, quoting from George Orwell’s classic novel, *1984*. He raised the concern that Consolidated’s restroom surveillance was a clear violation of California law and that collective bargaining agreements cannot contract for illegal activities.

3. ***Thompson v. Johnson County Community College*, No. 96-3223, 1997 U.S. App. LEXIS 5832 (10th Cir. March 25, 1997) (unpublished).**

Issue: Whether silent video surveillance of an employee locker area violated employee privacy rights?

Facts: Security officers at a community college had a locker area in a room that also housed the heating and air conditioning equipment for the college and which served as a storage area. Individuals other than the security officers could freely enter the room at any time. The room was not locked and access was not restricted to those with legitimate business in the room. The room was equipped with a silent video surveillance camera. The security officers alleged that the video surveillance violated

the Electronic Communications Privacy Act (ECPA) and their Fourth Amendment privacy rights.

Holding: The court held that silent video surveillance, i.e., video surveillance without audio capability, is not covered by the ECPA. Therefore, silent video surveillance did not violate the Act. Employees may be able to assert a right to privacy in their personal locker space, and other areas such as a locked desk, when adequate notice is not provided that such areas may be subject to unconsented searches. However, they do not have a reasonable expectation of privacy in the area surrounding a locker and other public or semi-public space. The fact that few people other than the security officers entered the room did not change the court's analysis.

4. ***Service Employees International Union, Local No. 152, AFL-CIO Racine Unified Sch. Dist., Case 191, No. 58280, MP-852.3.2, Dec. No. 29846-B (WERC, 2/2001).***

Issue: Whether the School District's decision to install and utilize hidden video cameras on the loading dock and in the break room for the purpose of theft detection was a permissive subject of bargaining?

Facts: The School District installed and used hidden video cameras on the loading dock and in the break room because of concerns with the need for theft detection. Neither camera recorded sound. The School District installed the hidden video cameras after complaints from a number of employees at an elementary school indicated that the building service employees were taking extended lunches and breaks, standing around a lot, and taking school lunches for free. The video cameras were installed at the loading dock and in the break room to investigate these allegations.

The Union found out about the video cameras and filed a complaint with the Wisconsin Employment Relations Commission (WERC), claiming the practice was primarily related to wages, hours, and terms and conditions of employment, specifically, job security. The Union also raised privacy concerns. The District claimed the hidden video cameras were a legitimate investigatory or information gathering tool used to safeguard District property or the health, safety and welfare of its employees and students. The Union did not request that the District bargain over either its decision to install and utilize hidden video cameras, or the impact of the District's decision.

The WERC Examiner found for the District. The Union then appealed to the Commission.

Holding: The Wisconsin Employment Relations Commission affirmed the WERC Examiner's finding that under the facts of this case the use of hidden video cameras was not a mandatory subject of bargaining within the meaning of Wis. Stat. § 111.70(3)4 or derivatively 1. The School District's decision to install and utilize hidden video cameras on the loading dock and in a break room to investigate allegations of employee misconduct primarily relates to the management and direction of the School District and the formulation or management of public policy.

The Commission distinguished the instant case from the employees/unions right to bargain for a disciplinary process which will give them notice of the employer's expectations for their job performance, notice when they are failing to meet those expectations, and opportunities to correct any performance deficiencies. Here, the misconduct in question was theft of property or time, and there are no issues of notice or knowledge of expectations. The Commission noted that the employees know they are not allowed to steal property or time.

5. ***Bohach v. The City of Reno, 932 F. Supp. 1232 (D. Nev. 1996).***

Issue: Whether the government department's retrieval of messages stored on the computer network violated federal wiretapping statutes and the employee's constitutional right to privacy?

Facts: The city police department used a software program that allowed the transmission of brief messages to visual display pagers. These are considered electronic communications that fall within federal law. An order issued by the chief of the department warned all users that every message was logged on the network, and that some types of messages were prohibited. The officers involved in the case sent messages to one another that were subsequently used during an internal affairs investigation against them. The officers claimed a violation of the Fourth Amendment prohibition against unreasonable searches.

Holding: The court found that the officers did not have an objectively reasonable expectation of privacy in the messages. To prevail on their claim, the officers had to demonstrate that they had a reasonable expectation of privacy in their use of the message system. The court distinguished between the transmission or transfer phase of the communication and the electronic storage of the messages. The court reasoned that the city was the "provider" of the "electronic communications service," including the computer terminals, computer and software, and the pagers issued to personnel. These items provide the user the ability to send or receive electronic communications. The law allows providers of these systems to access stored electronic communications.

B. Federal and State Legislation.

1. Electronic Communications Privacy Act of 2000 (ECPA) (Federal Wiretap Act) (18 U.S.C. § 2510-2521; Wis. Stat. § 968.31).

- a. It is unlawful to *intercept* and disclose wire, oral, or electronic communication, including telephone conversations and e-mail, while it is in transit.
- b. An electronic communication consists of the *transfer* of the signals, data, and other items, but does not include their electronic storage. Interception occurs when it is captured or re-directed in any way through the use of a mechanical or electronic device. This may include obtaining access to in-storage wire communications (e.g., obtaining access to someone's voice-mail mailbox and forwarding it to your own).
- c. Ordinary course of business exception: the employer is allowed to monitor or record employee communications if it is done for a legitimate purpose and all employees have been informed about the monitoring device. It may be limited, however, to determining whether the nature of the communication is business related. The employee must be given prior notice.
- d. Consent exception: It is not unlawful to intercept communications, such as e-mail and voice mail, while it is in transit if one party to the communication has given his or her consent to the interception. This may be inferred either through an employment contract or through a well disseminated e-mail policy.

2. Electronic Communications Privacy Act of 2000 (ECPA) (Stored Communications Act) (18 U.S.C. § 2701-2711).

- a. It is unlawful to access *stored* electronic communications, such as e-mail, pagers, and voice mail, while it is in electronic storage.
- b. Whoever intentionally accesses without authorization a facility through which an electronic communication service is provided or intentionally exceeds an authorization to access that facility, and thereby obtains, alters, or prevents authorized access to an electronic communication while it

is in electronic storage in such system shall be punished. Accessing e-mail from a stored database without authorization is prohibited, including read or sent e-mail that is saved on the user's server or hard drive.

- c. Provider exception: the prohibitions against accessing stored electronic communications do not apply to conduct authorized by the person or entity providing an electronic communications service. The provider is the entity that provides the terminals, computers, software, pagers, etc. Therefore, if an employee provides access to e-mail through an in house e-mail server, the employer is free to monitor an employee's stored e-mail. This may not apply if access to e-mail is provided through a commercial Internet service provided, such as America Online.
- d. User exception: the prohibition does not apply to users of the service with respect to a communication of or intended for that user. This exception includes individuals who expressly or impliedly have been given authorization to access the user's stored e-mail.
- e. Ordinary course of business exception: a person or entity may divulge the contents of a communication as authorized under § 2511(2)(a) (see previous section).
- f. Although the law is unclear regarding employer rights in this area, it is best to provide employees with prior notice of the employer's intent to monitor employee stored e-mail.

C. Privacy Rights: Employer Searches.

1. *United States v. Simons*, 206 F.3d 392 (4th Cir. 2000).

Issue: Whether a government employer conducted an unlawful search of materials received by an employee at his government workplace via the Internet when it suspected a violation of workplace rules?

Facts: The government agency instituted a policy regarding Internet usage by employees. It stated that employees were to use the Internet for official government business only. Accessing unlawful material was specifically prohibited. The policy also explained that the agency would conduct electronic audits to ensure compliance that consisted of periodic auditing, inspecting, and/or monitoring the user's Internet access as deemed appropriate (which included e-mail messages).

While examining the agency's firewall log, the system administrator discovered evidence that the employee was accessing child pornography sites while at work. The systems administrator had noticed that the log was unusually large, and searched the log using the keyword "sex." Because the search generated a large number of "hits" traceable to the employee's workstation, indicating intentional Internet searches (rather than casual or accidental), the supervisor had the systems administrator access the employee's workstation computer to see if the employee had downloaded any pornographic pictures or files. Over one thousand pornographic files had been downloaded. A criminal investigation was initiated and a search warrant was obtained for the employee's office, including the computer and contents of its drive. The employee was indicted on one count of knowingly receiving child pornography in violation of a federal criminal law. The employee moved to suppress the evidence because of an illegal search in violation of his Fourth Amendment rights.

Holding: The court held that the agency's policy limiting the Internet to official purposes and giving notice that audits may be done on unclassified networks was sufficient to eliminate any reasonable expectation of privacy the employee had regarding his Internet use. Additionally, the systems administrator had a duty to monitor Internet use, including inappropriate workplace activity, as part of his official duties. The searches, therefore, were not illegal.

IV. Acceptable Use Policies (AUPs).

A. Employee AUPs: Developing an Acceptable Use Policy.

1. Written Agreements.

Acceptable Use Policies, or "AUPs," often take the form of written agreements between employers and employees, and, at a minimum, set forth permissible uses of the Internet and e-mail.

2. Reasons for implementing an AUP.

- a.** To address/prevent lost productivity.
- b.** To provide a shield against liability.
- c.** To address technological and budgetary concerns.
- d.** To provide uniformity and fairness. All employees' expectations of privacy are equitably limited by AUP's. Also, discipline for inappropriate use can be more readily justified and evenly applied.

B. Non-Exhaustive Checklist of Elements for an AUP.

1. Purpose.

A purpose statement will often provide that the agreement is intended to identify the appropriate use of e-mail and the Internet, establish ownership of information, define the scope of technology covered, define limits of personal privacy, and state specific prohibitions. It should include a statement that the computers and their software are educational tools owned by the district. Limiting the use of the computer systems is advisable in order to reduce inappropriate use of the system. Further, it should establish rules regarding personal use of the district's computer system by students. Also, because school districts are responsible for public records under public records law, developing rules of conduct is advisable regarding technology.

2. Security Measures.

Security measures should include deciding who will have access to the computer systems. If all employees are not provided access, it is necessary identify which employees will have access; employees should be identified by job classification or another categorical system. Each employee should be given identification and personalized passwords. All users should be directed to limit their use and access to themselves.

3. Privacy Rights.

It is important to state clearly that Internet and e-mail communications are not private, but rather are subject to oversight by district officials. An employer may also warn employees that e-mail is significantly less secure than other traditional forms of communications because messages can be printed and backed-up on disk. If the school board decides to permit some personal use of its computer systems, it should still inform users that the district intends to conduct regular audits of the system which would result in searches of personal messages. Further, a school district that maintains a website may not use the site to obtain personally identifiable information without the consent of the person from whom the information is obtained.

4. Nondiscrimination and Sexual Harassment.

An AUP should contain a statement which is consistent with the employer's general policy on sexual harassment and discrimination. For example, a statement may provide that neither e-mail nor the Internet should be used to send jokes or other comments that may be discriminatory, harassing or offensive to others or material that defames an individual, company or business, or discloses personal information

without authorization. Penalties may include criminal sanctions under Wis. Stat. § 947.0125 for threatening, abusive, or intimidating messages sent to another person through e-mail or other computerized communication system. Employers should also advise that, while monitoring may occur, it is not possible to check and evaluate every communication and, therefore, employee reporting is essential to address harassment.

Provide notification, consistent with the employer's policy on sexual harassment, that employees are not to access pornographic sites or display images of a sexual nature on their monitors. Penalties for such use may include criminal sanctions under 18 U.S.C. § 2252 and Wis. Stat. §§ 948.11, 948.12.

5. Copyright Infringement.

An AUP should identify the unauthorized installation of software on the district's computer system as prohibited by the school district. Further, the district should prohibit unauthorized posting and copying of protected material consistent with the board's copyright policy.

6. Unacceptable Use Computer Systems.

When drafting an AUP, employers must determine what activities to prohibit, e.g., use for personal business, soliciting or lobbying for political or religious causes, use for unethical or disruptive activities, sending junk mail or chain letters for becoming a member of non-work related listserves. Other unacceptable uses would include physical damage or theft of equipment. Under the Municipal Employment Relations Act (MERA), an employer is prohibited from interfering, restraining, or coercing municipal employees in the exercise of their rights. If any action targets the prohibition of employee personal use of e-mail in only situations involving union activities, it would likely be in violation of the law. Whether restrictions would be prohibited would depend on the specific facts of each case. As long as the AUP is nondiscriminatory on its face and is applied in a consistent manner, it will be presumed to be valid.

7. Monitoring, Supervision, Enforcement, and Penalties.

Monitoring can be accomplished by installing computer monitoring software. Employees in charge of supervising student usage should understand that supervision is part of their job responsibilities, understand what uses are acceptable, and be put on notice of the administration's expectations. School officials should also develop a system of reporting violations. Lastly, the AUP should identify the penalties for violations of the rules set forth in the policy.

8. Acknowledgement By User of the AUP.

A consent form should accompany the policy, whereby a user acknowledges and agrees to the provisions of the AUP. The form should state that the user is consenting to the monitoring and access of both their e-mail and Internet usage.