



# SESSION TWO

## Technology Law Update

---

David R. Hostetler

*Lex-IS Services*

[www.Lex-IS.com](http://www.Lex-IS.com)

[Services@Lex-IS.com](mailto:Services@Lex-IS.com)

815-301-3931

# *School Cyberlaw*

## *Recent Cases and Legal News*

Winter 2010

David R. Hostetler, *Esq.*  
*Lex-IS Services*<sup>1</sup>

---

<sup>1</sup> Lex-IS Services, PO Box 3496, Chapel Hill, NC 27515 / 919-308-4652 / Services@Lex-IS / [www.Lex-IS.com](http://www.Lex-IS.com)

All information in these materials is for educational and information purposes only and not offered as legal advice. Formal legal counsel should be sought when addressing specific legal questions.  
Copyright 2009.

## **A. CyberSafety: Student and Employee Protection and Privacy**

### **“Sexting:” Parents of suicide student sue school district.**

A Cincinnati high school senior, Jessica Logan, sent a nude picture of herself to her boyfriend. After they broke up, he forwarded the picture to one of Jessica’s friends who then forwarded the picture to a wider circle. Jessica interviewed on NBC’s The Today Show to warn others about the dangers of sexting and, because students were aware, she became subject to further abuse. One month after graduating, she hangs herself in her closet.

The parents have filed a suit against the school and other individuals. They claim that school officials were negligent for failing to enforce its harassment policy. The parents sought the help of the guidance counselor who referred the matter to the school resource officer (a co-defendant) and, according to the complaint, the SRO stated that he could do nothing more than to ask the students to delete the pictures from their phone. When the parents sought to press charges, the prosecutor informed them that because she was eighteen, there were no child pornography laws to protect her. Source: [eSchool News Online](#), Dec. 10, 2009

### **“Sexting”: Court precludes criminal charges against student for “sexting” pictures through her cell phone. Miller v. George Skumanick (M.D.Pa. Apr. 3, 2009).**

A judge ordered a Pennsylvania district attorney from filing criminal pornography charges against female students after they sent pictures of themselves clad in their underwear via their cell phones. Officials at the girls’ school found pictures in several student cell phones of "scantily clad, semi-nude and nude teenage girls” and turned the phones over to the district attorney. The parents, in this case, successfully contended that the images did not constitute child pornography since they did not depict sexual activity or show the girls' genitalia. The district attorney had demanded in lieu of being criminally charged, that the girls attend a "re-education" program and write essays about their improper conduct. The parents successfully argued that such a requirement violated their due process rights to educate their children. Source: Westlaw Watch, April 16, 2009.

### **Student Safety: FTC releases student online safety booklet.**

The Federal Trade Commission (FTC), on December 15, 2009, released the booklet, "Net Cetera: Chatting with Kids About Being Online," to help parents and educators instruct children on safe use of the internet and cell phones, including topics on cyberbullying and protecting home computers as well as conducting themselves properly while communicating with others. The booklet is available [online at the FTC website](#).

### **Federal Child Protections: Child Online Protection Act struck down again by Third Circuit Court of Appeals. ACLU v. Mukasey, No. 07-2539 (3d Cir. July 22, 2008).**

The Third Circuit Court of Appeals ruled that the federal Child Online Protection Act (COPA) was unconstitutional because of First Amendment free speech violations. COPA dates back over a decade and has undergone much litigation. The United States Supreme Court previously overturned a 2002 Third Circuit ruling that COPA’s “contemporary community standards” was overbroad in determining if online materials were harmful to minors. Subsequently, the

Supreme Court upheld a district court preliminary injunction preventing COPA's enforcement because less restrictive methods existed to achieve its goal of protecting minors from harmful Internet content.

In the present case, the Third Circuit held that the federal government failed to satisfy its burden of proof "that COPA is a more effective and less restrictive alternative to the use of Internet filters..." in accomplishing its objectives. (In this instance the government must find the least restrictive means of doing so since free speech rights are placed in jeopardy.) Thus, despite the government having a "compelling interest" in preventing minors from viewing harmful material online, COPA was too broad and restricted online content that "adults have a constitutional right to receive."

### **Social Networking: congress passes new Internet safety law.**

Congress recently passed the "Protecting Children in the 21<sup>st</sup> Century Act" as part of a larger bill dealing with broadband access. The child protection provisions call for a nationwide collaborative effort directed by the Federal Trade Commission (FTC) to increase public awareness and provide education on effective strategies that promote safe use of the Internet by children. The Act also calls for annual reporting of such efforts and establishing an "Online Safety and Technology" working group to study and assess the national efforts and technologies designed to improve child safety. In addition, each school applying for federal E-rate funding (pursuant to the Children's Internet Protection Act) must additionally certify that

"as part of its internet safety policy [it] is educating students about appropriate online behavior, including interacting with other individuals on social networking websites and in chatrooms and cyberbullying awareness and response."

### **Social Networking: As troubling online video postings of teen violence increase, schools contemplate how to fight back.**

YouTube and websites like it that allow users to post self-made video content have become repositories for a great deal of video depicting teen violence. Some of the videos are created spontaneously when inevitable schoolyard fights break out, but more troubling are the videos that demonstrate premeditation, such as the beating of an unsuspecting teenager last year in Florida. Officials fear these videos, which are quite popular online and can draw over a million viewings, are glamorizing violence and will encourage even more such behavior.

Ironically, some school officials have used YouTube as a tool to identify and punish students involved in fights that they might not otherwise have detected, a task made easier when identifying information like school names are posted with the videos. A few schools have even added rules to their student policy manuals banning the recording of fights, with violators being subject to punishment, including suspension. Finally, elected officials in California's state government have proposed a new state law that would require YouTube and similar websites to actively search for and remove violent video content. YouTube currently employs a user enforcement procedure whereby any user can 'flag' a video for "graphic or gratuitous violence." The company then reviews flagged videos for rules violations and potential removal. Source: [e-School News](#), March 19, 2009.

## **Student Privacy: School system mistakenly publishes students' social security numbers.**

Parents of about 5000 Wake County students were startled to receive postcard school calendar selection reminders sent through the postal mail containing student social security numbers plainly printed on the front of the cards. The system's database incorrectly included the numbers based on an apparent database glitch. The school system has offered one year of free credit reporting service to the affected households, costing close to \$100,000. Source: [Raleigh News & Observer](#), Dec. 5, 2009.

**Employee Privacy: U.S. Supreme Court to review case involving employee privacy protections in text messages.** Quon v. Arch Wireless, No. 07-55282 (9th Cir. June 18, 2008); cert. granted, City of Ontario v. Quon (U.S., Dec. 14, 2009).

The U.S. Supreme Court will hear and decide a case of special significance in the area of technology use and employee privacy. The case was decided previously by the Ninth Circuit Court of Appeals, making it much more difficult for public employers within that jurisdiction to access the text messages sent by their employees through a private provider's network because employees may have a reasonable expectation of privacy in the messages they send.

The case involved members of the Ontario (Cal.) Police Department ("OPD") using their department-issued wireless pagers for personal text messaging in excess of their allotted usage plans. The OPD had purchased pagers for their employees with text-messaging capabilities and services (the "Plan") from a private provider. Text messages were sent and received via the pagers and transmitted and stored in the provider's computer network. City policy, under which the OPD operated, had no specific text-message or pager policy. Its "Computer, Internet, and E-mail Policy," however, was broadly worded to include a number of computer and network-related equipment. That policy explicitly prohibited personal use of such equipment and notified employees of the city's right to control, monitor, and search any device covered by the policy. It also stated that employees had "no expectation of privacy" and no right to confidentiality in their use. The OCD supervisors communicated to employees that use of the pager text messaging was considered "e-mail" under the city policy.

The plaintiffs, on several occasions, exceeded their pager use limits under the Plan. They were informed that as long as they paid the overage charges, the OCD would not inspect their pager messages to determine if the overages were a result of personal use. Eventually the OCD conducted its audit to examine the cause of the overages. The service provider, therefore, supplied a hardcopy to the OCD of plaintiffs' text messages. Those records indicated that the plaintiffs used their pagers for extensive personal use, including the sending and receiving of sexually explicit content.

The plaintiffs sued the OCD, the city, several city officials, and the service provider, claiming that the city violated their Fourth Amendment protections against unreasonable searches and that the service provider violated the federal Stored Communications Act of 1986 – a part of the Electronic Communications Privacy Act – by disclosing plaintiffs' pager use records to the city without the plaintiffs' consent.

Regarding the Stored Communications Act claims, the court ruled that the service provider violated the law by not obtaining consent from the plaintiffs, despite the fact that the city was the account subscriber. Regarding the Fourth Amendment claim, the court noted

The extent to which the Fourth Amendment provides protection for the contents of electronic communications in the Internet age is an open question. The recently minted standard of electronic communication via e-mails, text messages, and other means is a new frontier in Fourth Amendment jurisprudence that has been little explored.

The court declared that users have a reasonable expectation of privacy in their records stored on a private service provider's network. Despite the city's broadly worded e-mail policy, the court noted that the city had never previously monitored or audited pager text messages. In addition, the plaintiffs had always been allowed to pay their overage charges in lieu of having their messages audited. These practices instilled an expectation that such messages were private, despite formal policies and pronouncements to the contrary. Furthermore, ruled the court, the scope of the city's search of records was also unreasonable since there were other simpler ways it could address the problem of Plan overages.

Finally, the court did rule that city officials were immune from liability in their individual capacities. Even though the plaintiffs' rights were violated, those rights were not so "clearly established" that city officials could reasonably know that.

**Lex-IS Notes:**

- Remember, this case is not binding on North Carolina schools until the Supreme Court renders its decision. Whether its employee-friendly and liberal constitutional interpretation would be upheld in this jurisdiction is highly questionable.
- Such cases are very fact specific; even the court notes that its ruling can not be broadly applied.
- The court's ruling raises a number of practical concerns for government employers. For example, use of private electronic service providers may broaden an employee's Fourth Amendment rights. Also, despite broad and explicit policies and pronouncements declaring no employee expectation of privacy in electronic communications, failure to periodically notify and implement monitoring efforts may increasingly create an "expectation of privacy."
- Unfortunately, the court's ruling could lead employers, at least in the 9<sup>th</sup> Circuit, to start monitoring and reviewing employee communications when there is no apparent need to do so simply to address the court's point regarding an employer's right to monitor and search: i.e., "if you don't use it, you lose it." In other words, an employer's failure to do what it has the right to do – i.e., search employee communications – could lull employees into expecting privacy and therefore produce a Fourth Amendment right.
- School attorneys should review school system policies and practices for consistency.

**Employee Privacy: Connecticut court determines principal had reasonable expectation of privacy in her school email account.** *Brown-Criscuolo v. Wolfe*, No. 3:05CV01486 (Conn. March 9, 2009).

A Connecticut district court found that a school principal had a reasonable expectation of privacy in her email, including an email and attachment she sent to her attorney describing problems she was having with the school superintendent. While the principal was on medical leave, the superintendent accessed the principal's email account and forwarded the email and attached letter she had previously sent to her attorney to his email account in violation of her Fourth Amendment rights against unreasonable searches.

The court also found that the principal's use of her computer to draft and send the letter was within the school's Acceptable Use Policy (AUP), which restricted use of school computers to professional or career development-related uses. Additionally, while the AUP also permitted routine monitoring and maintenance of the computer system, the court did not believe the superintendent's actions qualified as such.

**Social Networking: student posts his suicide online while others observe.**

Abraham Biggs, a 19-year old bipolar college student in Florida, committed suicide by drug overdose in front of an online audience that watched his death live via webcam. Viewers could "tune in" during a 12-hour period prior to, during, and after the death, and could post text comments. Eventually a user notified web host officials who tracked down the location and notified police who found Biggs after it was too late. The news report states that some online users encouraged Biggs to go through with it, some tried to persuade him to stop, and others did not realize it was anything more than a prank until his death was apparent, to which at least one viewer posted her reaction in horror: "OMG." One popular culture expert noted how common such public displays of intimate details are becoming, stating "If it's not recorded or documented, then it doesn't even seem worthwhile. For today's generation, it might seem, 'What's the point of doing it if everyone isn't going to see it?' " Source: News and Observer (AP), Nov. 22, 2008.

**Social Networking: Social websites potentially problematic for job applicants and employees.**

Social websites are growing in popularity. Increasingly, employers and others are searching these sites to gather information about job applicants and other people of interest. Teachers in the Charlotte School System, Durham police officers, and a college football player are just some of the recent examples of individuals suffering the consequences of such postings. One report indicates that over 70 million users have registered for Facebook accounts this year alone; a remarkable fact given Facebook's introduction just five years ago. Source: Raleigh News & Observer, Nov. 18, 2008.

**Social Networking: Recent study reveals some benefits to teen online social networking**

A recent study of 800 students and parents examining 5000 hours of social networking use revealed that the extent of some perceived dangers and downsides of social networking may be overblown and that we may have confused notions about how many students are using these sites. Essentially, the study describes how teens are using social networking sites; however, it cautions that little evidence exists to gauge the long-term effects. The study highlighted the literary, technological, and socialization benefits social networking sites offer, and confirmed teen habits of weaving networking into their daily routines, often beginning and ending their days with such use. The study showed teens using these sites to learn from one another or groups of like-minded individuals, developing skills in setting up a web site and presenting themselves, learning to interact with one another, and respecting others' interests. Source: Raleigh News & Observer (N.Y Times), Nov. 20, 2008.

### **Social Networking: Intervention aimed at encouraging more responsible use of MySpace shows promise.**

Two investigations aimed at understanding how 18-20 year olds used the social networking site MySpace yielded simultaneously startling and encouraging news. The most startling aspect of the research revealed that the MySpace pages of more than one-half of users in this age group contained references, often explicit in nature, to risky behaviors like sex, drinking, and violence. For example, researchers found public accounts of losing one's virginity and how one could increase their chance of having sex with another user (e.g., 'bring flowers and take me to dinner').

On the other hand, researchers were encouraged by the responses they received to simple email messages sent to MySpace users from "Dr. Meg" informing them that their on-line references to risky behaviors had been noticed and suggesting that the user reconsider making such information available to the general public via MySpace. Three months after sending the emails, 42% of recipients had removed the references to sex or drinking or changed their profiles to private compared to just 29% of those users who did not receive the emails. Source: e-School News.com, Jan. 7, 2009.

### **Privacy: Digital identification services present challenging dilemmas to schools.**

As child safety advocates seek new and improved ways to keep children safe online, a method known as "digital identification" has sparked controversy among some school officials. eGuardian, a new digital identification provider, claims its product keeps children safe by communicating with search engines and social networking sites and preventing children from accessing inappropriate content based on their age. The controversy stems primarily from eGuardian's use of school systems to verify information provided to it by parents who purchase the online child protection system. In essence, eGuardian pays schools to verify the information subscribers submit about their children. eGuardian also actively seeks to partner with schools, promising the school \$13 of the \$29 registration fee for each child subscribed.

Some school officials, though, are hesitant to become involved in any process whereby the school divulges student information to third parties, even in the name of online student safety. One skeptical official stated, "[s]chool systems need to ensure that student information is kept private as required by the Family Education Rights and Privacy Act. Parents can make individual choices if they wish to use digital ID software without school involvement." Source: eSchool News Online, Nov. 17, 2008.

### **CyberSafety: Student security concerns accompany online courses.**

As schools seek to simultaneously enhance course offerings and trim budgets, online courses have become increasingly popular. However, this has also sparked concerns about the online safety of students enrolled in such classes. Source: eSchool News Online, Nov. 17, 2008.

### **Personnel: charges result in North Carolina Central University firings.**

Three state employees at NCCU were fired for allegedly using university computers to download pornography and other improper material from the Internet according to the North Carolina State Auditor. Source: Raleigh News & Observer, June 18, 2008.

**Personnel Privacy: Teacher's privacy rights not violated by proposed audio monitoring of classroom.** Plock v. BoE. of Freeport Sch. Dist. No. 145, 07-C-50060, (N.D. Ill. Dec. 18, 2007).

A federal district court ruled that a school district's plan to audio record certain classrooms did not violate a special education teacher's Fourth Amendment claim because the teacher had no expectation of privacy in her classroom. Given the information regularly disseminated by students, plus the school's interest in classroom activities, a teacher's expectation of privacy would be unreasonable.

## **B. CyberSpeech**

**Forums: California community college may restrict Internet use on library computers to educational and employment uses.** Crosby v. S. Orange County Cmty. Coll. Dist., No. G040033 (Cal. Ct. App. Feb. 18, 2009).

The California Court of Appeals upheld a community college's policy which limited the use of library computers for accessing the Internet except for educational or employment purposes. The court found this restriction did not conflict with a state statute prohibiting schools from punishing students for actions in violation of school rules that would otherwise be protected by the First Amendment because the school's library computers were not part of a public forum.

**Students: Fake teacher and school administrator MySpace pages posted by students not protected as parodies.** Barnett ex rel. Barnett v. Tipton County Bd. of Educ., No. 07-2055-JPM-dkv (Tenn. Jan. 26, 2008).

A group of high school students in Tennessee created fake Internet profiles for a teacher/coach and assistant principal at their school and posted them on the social networking site, MySpace. The profiles, which were accessible to the general public, contained sexually suggestive comments about female students that appeared to have been posted by the school employees. The students claimed their websites were parodies and therefore protected by the First Amendment. However, the court held that the profiles were not parodies because they were reasonably believable (in fact, the school received calls about the postings from concerned community members) and were not clearly exaggerated to enhance humor.)

**Government Speech: Fourth Circuit upholds school system's right to exclude opposing policy viewpoints on its website and e-mail.** Page v. Lexington County Sch. Dist. One, No. 07-1697 (4th Cir. Jun. 23, 2008).

School Cyberlaw cases are growing in number as technology use expands. Still, few cases have been decided by federal appellate courts and fewer still by the Fourth Circuit Court of Appeals, which has jurisdiction over North and South Carolina schools. When they are, they are worth noting, especially when they address a significant area of law like the First Amendment as applied to school systems' use and control of their web pages and e-mail.

On June 23, the Fourth Circuit upheld the right of a South Carolina school system to deny a citizen "equal access" to the System's webpage, e-mail, and other communication mechanisms in

order to prevent that person from using those forums for supporting proposed voucher legislation. The school board for the Lexington County School District One (the "District") decided to oppose proposed state voucher legislation and to communicate its opposition through its webpage, e-mail, PTA newsletter and other channels.

The plaintiff supported the voucher legislation and requested that the District grant him "equal access" to its communications channels to advocate his pro-legislation views. The District refused and the plaintiff sued, claiming the denial was unconstitutional "viewpoint discrimination" under the First Amendment Free Speech Clause.

The federal district court granted summary judgment for the District (i.e., decided the case without a trial). The Fourth Circuit affirmed that decision in all respects. The court first addressed whether the System's policy advocacy against the voucher legislation was "government speech" and therefore exempt from First Amendment scrutiny. Reviewing the law of government speech, the court noted that the determination depends on the extent of the government's ownership and control of the message. Key factors include the speech's purpose, the extent of the government's "editorial control," the "identity" of the person making the speech, and the person having "ultimate control" over the content.

Applying each of those factors, the court determined that the System's advocacy was, indeed, "government speech." The Board decided to oppose the legislation and to communicate that opposition to the school and public community. At all points in time it controlled what content was conveyed. Even though some private party information was referenced or distributed, the decision to do so remained in the sole control of school officials.

The plaintiff argued that by linking to third-party information on the System's website, the District had created a "limited public forum," thus entitling members of the public, like the plaintiff, to have their views posted as well. The court rejected this argument. Its reasoning is particularly significant and instructive for school systems regarding website content and control. Key factors that kept the District's website "closed" included: (1) the fact that third-party websites were linked only based on their support of the District's position; (2) the District retained complete control of its own website, including the ability to delete any link at any time; (3) the District never adopted the third-party information as its own and it also included disclaimers regarding the content of third-party websites; and (4) the District never wavered in its opposition to the voucher legislation and its message was therefore consistent. In sum, the System "sufficiently controlled [its website] so that its speech remained government speech and it did not create a limited public forum by including links to other websites." The court ruled similarly regarding the System's e-mail communications.

Regarding the PTA newsletters, the court recognized that these may have created a limited public forum but that the plaintiff was not a member of the class of individuals entitled to provide content and that the District's regulations for the newsletter were reasonable.

Finally, the court upheld the District's right to advocate its policy positions. Rejecting the plaintiff's argument against this, the court noted that citizens had the right to vote school board members out of office if they did not like the board's advocacy. The court recognized the board's right to "defend public education in the face of pending legislation that it views as potentially threatening of public education."

**Lex-IS Notes:**

- There is a fine line between when a school system website or other forum is “closed” and when it is a “limited public forum” subject to public participation; school officials have often crossed the line without knowing it and therefore subjected their actions to greater First Amendment scrutiny.
- The factors applied by the Fourth Circuit in the Page case provide some guidance as to how a school system can retain control over the messages it communicates.
- Before making decisions about expanding or changing technology use, be sure to consider the First Amendment and other legal ramifications and get legal advice if there is question.
- School system policies should be reviewed periodically to determine if they comport with current technological and legal trends.

**Employee Speech: Fourth Circuit rules that employee’s work e-mail forwarding civil rights materials is not protected speech.** *Bowers v. Scurry* (4<sup>th</sup> Cir. May 2, 2008). [unpublished]

A University of Virginia human resource employee used her university e-mail to forward NAACP material in opposition to a school pay restructuring plan. The university fired the employee contending that the e-mail implied that it was an official HR communication, causing confusion to employees. The university had a policy that limited the sending of personal e-mails. In the employee’s resulting First Amendment lawsuit, the Court upheld the university action. Although the employee had a legitimate interest in communicating on a matter of public concern, the university’s interest in maintaining an efficient workplace prevailed.

**Religious Establishment: School website containing link to anti-homosexuality websites was permissible.** *Harper ex rel. Harper v. Poway Unified School Dist.* 545 F. Supp. 2d 1072 (S.D. Cal.) [Appeal vacated as moot, 318 Fed. Appx. 540 (9<sup>th</sup> Cir. Mar. 10, 2009)].

A federal district court in California ruled that a school webpage that included links to religious websites opposing homosexuality did not violate the First Amendment Establishment Clause. The plaintiffs failed to prove that the links did not fulfill a secular educational purpose or effect or that the links excessively entangled the school with religion. The court noted that a student had previously been disciplined for wearing an anti-homosexuality t-shirt, showing that the district was not pursuing a religious agenda.

**Student Speech: High school student suspended for Facebook posting about teacher.**

A Florida charter high school student sued her principal after being suspended after posting to her Facebook page a picture of a teacher she described as “the worst teacher I’ve ever met.” The principal suspended the student for three days for actions he deemed ‘cyberbullying harassment towards a staff member’ and ‘disruptive behavior.’

Attorneys for the student countered by claiming the Facebook posting was protected First Amendment speech because it occurred off campus, was devoid of threats of violence, and did not disrupt school activities. The student’s suit sought the revocation of the three day suspension from her permanent record. Source: NSBA Legal Clips, Dec. 11, 2008.

## **Employee Speech—Social Networking: Charlotte teachers’ Facebook posts result in disciplinary action.**

Several teachers in the Charlotte-Mecklenburg school system have been investigated and some disciplined for posting inappropriate images and material on social networking sites like Facebook. For example, a black teacher used the “N” word, several teachers posted images of themselves in sexually suggestive poses, one teacher referred to her school as “the most ghetto school in Charlotte” and to her students as “chitlins,” and a special education teacher stated, “I hate my students!”

Some of the teachers were suspended with pay pending investigation. Some faced dismissal for violations, in part, of the district’s code of conduct prohibiting “unethical or lascivious conduct,” and others faced lesser disciplinary actions. The district reports that it must address these types of problems each year. It was sending a memo to all 19,000 of its employees reminding them of appropriate personal web practices. Source: Charlotte Observer, Nov. 12, 2008.

## **C. CyberSystems**

### **Record Retention: New law requires additional attention to archiving email.**

A December 2006 change in the Federal Rules of Civil Procedure required school district email and instant messages to be included in the discovery process pursuant to federal lawsuits. Despite this change, recent studies suggest that as many as 90 percent of schools have not implemented appropriate digital archiving technologies to satisfy the discovery requests that would accompany a lawsuit in which the school was involved.

The Consortium for School Networking has released a paper that it hopes will enlighten school officials on what they should know, how they should approach digital archiving, and what other schools are doing to address the archiving requirements. Source: eSchoolNews.com, July 2, 2008.

### **E-Mail: New Jersey court bars school board candidates from soliciting support via school system e-mail.**

According to a recent news report, a New Jersey state court issued a cease and desist order to two board candidates from using school system e-mail server to solicit support from system employees. The candidates purportedly obtained the staff e-mails from the school web site. The system’s technology policy prohibits staff from using the system’s network to assist with “a campaign for election of any person to any office or for the promotion of or opposition to any ballot proposition.” The provision applies to anyone using the system’s mail server. [Source: Asbury Park Press](#), Mar. 24, 2009.

## **D. CyberSchooling**

### **Ethics: GMAT test cracking down on online cheaters.**

About 6,000 Graduate Management Admission Test (GMAT) scores are in question following a recent court ruling against an online website that contained previews of current questions on the standardized admission test for graduate management programs. GMAT officials are currently in the process of identifying the individuals who accessed the website and will cancel the scores of those who did. It remains uncertain how graduate programs will handle suspected cheaters, especially those already enrolled in classes. Source: eCampusNews.com, July 15, 2008.

### **Instruction: Digital assessment use can be greatly improved.**

While schools have markedly increased their use of technology to provide new learning tools to students and to protect student data, a recent survey by the Software and Information Industry Association (SIAA) indicates that schools are still not using digital assessments to their fullest potential. The SIAA, whose Vision for K-20 Education provides a “framework for using technology to transform education,” advocates the use of computer-based adaptive testing as a way to more accurately pinpoint the strengths and weaknesses of individual students. Source: eCampusNews.com, July 15, 2008.

## **E. CyberSecurity**

### **Network Security – Spam: Spam celebrates 30 years of clogging e-mail inboxes.**

A recent news report reminds readers of the birth of e-mail “spam” 30 years ago when computer salesman Gary Thuerk, on May 3, 1978, distributed a message on Arapanet, the precursor to the internet, that read: "We invite you to come see the [Computer System] 2020 and hear about the DECSYSTEM-20 family at the two product presentations we will be giving in California this month."

The message produced a backlash from academic and government users of the system. The article cites Microsoft founder Bill Gates' 2004 prediction that spam would soon be eliminated. This year also marks the 10-year anniversary of the first Viagra spam e-mail; one such early message offered a bottle of 30 pills for \$500.00. Real spam, not the virtual kind, celebrated its 70<sup>th</sup> birthday last year. Raleigh News & Observer, May 3, 2008 (from the Washington Post).

### **Network Integrity: Computer hackers targeting school system computers to launch attacks.**

Opportunistic cyber criminals are constantly looking for large computer networks that are relatively free from security to launch their attacks, and education institutions are often prime targets. Seeking to make it easy for students and faculty to access on-line educational resources, schools and universities often provide little protection, if any, to their computer systems. Consequently, hackers are able to essentially take over the system, or parts of it, and turn it into a “botnet” to launch anonymous spam or virus attacks that can cripple an entire computer system if undetected. Technology departments are encouraged to constantly monitor school system

firewalls and spyware and to ensure updates and security patches are installed in a timely manner. Source: eCampusNews.com, July 15, 2008

**N.C. Community College server hacked.**

The 25-college North Carolina Community College system, in December 2009, notified individuals that approximately 51,000 confidential user records were subject to a hacking attack in August 2009. The hackers apparently decoded a user password to a Raleigh server. Source: [WRAL](#), Dec. 18, 2009.