PART V

SUPREME COURT OF THE
STATE OF NEW YORK

CRIMINAL DIVISION

THE PEOPLE OF THE)
STATE OF NEW YORK)
)
v.) Case No. MT-00
)
MICKEY JACKSON, DEFENDANT)

STATEMENT OF STIPULATED FACTS*

Silas Cone High School of the East Bay School District has a widely recognized dedication to the procurement and application of cutting edge computer resources to support teaching innovations and student achievement. This community supported policy includes the creation of a faculty-directed student computer support group, Student Learning via Integrated Computer Services (known as SLICS) which has played a leading role in designing, implementing, and maintaining the district's computer network and related services. The faculty advisor, Val Watson, oversees the efforts of over 45 students. SLICS members researched computers to be purchased, installed hardware and software, partnered with community volunteers led by Randy Ruiz to wire the district's schools for Internet access during the summers of 1998 and 1999, and provided ongoing maintenance and technical assistance to users. SLICS was integrated into the district's technology education curriculum, which was broadly conceived and focused not only on the technical "how-to's", but the wider societal implications of technological innovation. SLICS students assisted as classroom tutors in the K-8 program and helped design and demonstrate lessons focused on computer use, the life implications of computer skills, and computer-induced economic and societal changes.

A significant dispute arose during the 1998-99 academic year between the high school administration and the faculty, supported by SLICS and other students, over the too restrictive nature of Internet filters in place on the school's Internet access. Biology teachers had complained that most of the human body, and associated diseases, were off limits; social studies teachers that current events, if at all violent, or constitutional but related to the president's impeachment trial were inaccessible; journalism classes couldn't access the pages of major news magazines or newspapers; and the list went on. Ultimately, in March, the school board agreed to allow individual high school teachers to set and rely on the filters available on individual machines, rather than on one restrictive filter set to control K-12 access.

Principal Dean and Vice Principal Martinez had expressed displeasure to Val Watson concerning the aggressive lobbying efforts of some members of SLICS concerning the filter issue. Three students, including Mickey Jackson, were called into the vice principal's office after they carried picket signs, on school property, on the night of the high school's winter music concert, and were told that they would be disciplined for future such behavior.

During the spring of 1999 several violent incidents at schools across the nation affected the district's attitude toward its recent decision on student Internet access and filters. Concerned about safety and liability issues, Dr. Dean urged the superintendent, and the superintendent then urged the board, to revisit the recent filter decision and to update its Acceptable Use Policy (AUP) to predicate access rights on students' and parents' agreement to monitor student home pages for unacceptable violent, hate filled, or pornographic tendencies. While the board shared the safety concerns, they were unwilling to publicly reopen the filter debate. They did, however, create a technology subcommittee to further investigate the safety and liability issues that might arise if the district's "flexible" filter program proved ineffective. That subcommittee, which included Dr. Dean, reported in June, 1999 that the district could best protect itself from potential liability and best monitor teacher-set filters and student adherence to the district's AUP by installing a special "buffer" computer, known as a proxy server, to audit and record all Internet usage. While not restricting access to proscribed sites—and thus being invisible to the normal user—its record keeping ability would allow the district to pinpoint misuse and intervene appropriately to maintain student discipline and safety. The board accepted this recommendation and voted to spend funds budgeted for ongoing computer upgrades to purchase and install the new buffer hardware server and software. A local computer vendor, D.R.I., was contracted to do the work, which was completed in mid-August, 1999.

In early September Mickey Jackson, known as "Speed" because of remarkably quick computer abilities, and a few other senior members of SLICS called their advisor, Val Watson, inquiring about when they could come in to install the ten new research computers scheduled to be purchased over the summer for use in the school library. Watson knew that the purchase of those machines had been delayed and told the students that the district spent those funds on other computing needs. Following this, Mickey Jackson posted a very critical essay on his personal computer's home page, questioning why and how the district could reappropriate computer funds away from a student-centered use and why Val Watson, and SLICS, had not been given any input into the decision or asked to assist with the unknown "other computing needs." Mickey and three other members of SLICS attended the next school board meeting and questioned the board's decision but received no detailed explanation.

At the same time that this was unfolding, Val Watson received a number of inquiries from teachers asking about possible changes in the Internet setup over the summer. A few noted that their classes that came later in the day didn't seem to have the same good results on basic searches as earlier classes—one journalism teacher specifically pointed out that the later class's news requests took them to the same pages that the first period class had accessed, not the later, current home pages. Watson promised that SLICS would look into it.

Watson asked Mickey Jackson to choose one younger student to help and to look into this problem. Jackson chose A. J. Gates, a sophomore, and the two stayed after school on September 20 and 21 to check out the system. Initially they sought to recreate the seeming anomaly by visiting various news sites from the affected classrooms. They also got the same unexpectedly "old" webpages the first afternoon. Jackson came in early the next day to again test the Internet results. At that time, the system worked as expected, allowing access to real time news postings, just as teachers had reported.

Jackson shared this information with Val Watson, who said that he would check with the administration about any potential changes to the system. Watson spoke to Principal Dean about Internet changes and was told that nothing had been done over the summer that would cause such a problem. Based on this, Watson told Jackson to proceed with the "hunt" for an answer. Jackson and Gates spent the second afternoon in a systems check of the school's Internet configuration, using the system administrator's password to gain access. They quickly realized that the system had been shifted through a new proxy server and accessed that computer's software and configurations, finding that the daily problems described by teachers were the result of the chosen default settings—the new server automatically checked to see if a site had been requested in the past 12 hours; if it had been then it provided that site from its cache file, not seeking the site from the Internet again.

While surprised by the existence of this server, Jackson and Gates were shocked by the "use records" folder, which maintained a record of all Internet usage, with coinciding user codes and computer identifying numbers. The user codes were confidential; the computer I.D. numbers were already in the possession of SLICS because of their installation and service duties. To demonstrate the setup, Jackson referenced the known computer I.D. numbers, searched for the usage records of the principal and vice principal, found these, and printed them out, all on September 21.

The students shared this information and the printouts with Watson the next day. Jackson, having had an evening to think about normally confidential usage records being kept in a not perfectly secure folder, determined to make a public issue of the school's actions. Val Watson was personally disappointed, given the significant teaching and volunteer work that had gone into making the district's students knowledgeable about technology and privacy issues, that such sensitive records were allowed to exist in a place with relatively easy access rather than behind a secure "fire-wall-like" barrier to preserve confidentiality, as was the case with other private records such as student grades.

Val Watson promised to pursue these issues with the administration and advised them not to visit the proxy server in the interim. "Speed" Jackson decided to bring the issue to a head by demonstrating the new system's threat to privacy. Jackson, having taken the copy of the user history printout home the night before, had begun checking on the sites visited by the administrators, making notes of what was found. The following evening Speed composed an essay about the school's Internet changes, entitling it "Hypocrisy.org and Incompetence.com", attacking the school for its secret changes and the contracted vendor for its "botched" setup.

Jackson warned students that they should be aware that their every move was being recorded on an "unsecure system." Jackson also wrote a second story entitled, "Guess Who's Going Where?" that purported to describe a "frustrated administrator's" Internet visits, and posted both stories on a home webpage.

The next day, September 23, Speed told several members of SLICS to look at that home page, including A. J. Gates. Gates and the others were impressed with what they read and started making jokes about the administrator's choice of websites. Gates also, from home, sent an e-mail via several school listserves (set up by teachers to disseminate information and assist students with homework and research assignments) reaching students in A. J.'s classes, touting the postings on Speed's website.

On Friday, September 24, the school was abuzz with discussions about the district's Internet changes and with ridicule and jokes directed at the principal, the assumed target of the "Guess Who's Going Where?" posting. Several teachers informed the administration of students' comments, of having received the e-mail from A. J. Gates, and of numerous students refusing to take part in Internet assignments while their every move was open to scrutiny.

Dean called A. J. Gates to the office. Gates admitted sending the e-mail, but denied having "broken into" the school's computer system. The principal, warning Gates to be forthright or face suspension, asked if any changes had been made to the system. Gates responded that Jackson had made at least one, but was moving so fast that there might have been others. Gates vowed total cooperation, saying that "I didn't do anything wrong."

Dr. Dean then called the district's business manager, Terry Wagner, and expressed concern that the integrity of the new buffer computer might have been compromised, given student access and the negative reaction of the involved SLICS students. Dean suggested getting the computer vendor back to recheck the system. Wagner called D.R.I. and spoke to Pat Chang, who agreed to check out the system on the following Monday, September 27. After inspecting the Internet computer system, Chang reported that the default settings had indeed been changed, so that every Internet request now actually went out to retrieve a "new" file. Further, the Internet usage folder had been disabled as of 12:05 a.m on the 24th, so that no ongoing records were being created. Finally, the September records had been deleted, as of noon on Friday, September 24. Dean asked Chang if any of these acts were criminal and was told that they certainly were if unauthorized.

Based on this information Dr. Dean called the East Bay Police Department on the afternoon of September 27, reporting on the whole situation. That evening, Mickey Jackson was arrested and charged with three crimes: 1) unauthorized use of a computer, in violation of N.Y.P.L. § 156.05; 2) computer trespass, in violation of N.Y.P.L. § 156.10; and 3) computer tampering in the fourth degree, in violation of N.Y.P.L. § 156.20. The criminal information alleges that Mickey Jackson broke into the school's computer system, downloaded secure data on Internet usage, and then posted writings based on that information on a home website. The school principal further alleges that Jackson disabled the school's Internet proxy server, preventing it from recording individual usage and deleted existing usage records. The principal claims that these actions created a safety hazard for the district, were motivated by a desire to embarrass the principal and vice-principal, substantially disrupted the educational process and school discipline, and undermined a safe and effective learning environment.

Mickey Jackson disputes the factual basis of these charges. Jackson argues that the school district created the problem when it "secretly" installed a "buffer" computer to track all Internet usage, thereby acting in bad faith; that the district improperly failed to protect the reasonable privacy rights of Internet users within the school by not securing the usage data but in fact allowed easy access to it by many people; and that such arrest infringes upon a student's constitutionally protected right to free speech on a home-based website. Jackson further claims that the only actions taken with regard to school computers were authorized by SLICS advisor Val Watson and that the only changes to the school's computer settings were within the scope of Watson's directives.

WITNESSES

FOR THE PROSECUTION

Chris Dean, Ed.D.
Principal

Pat Chang
Computer Consultant, D.R.I.

A. J. Gates
Student, Member of SLICS

FOR THE DEFENSE

Mickey Jackson
Student

Val Watson
Computer Science Teacher and
Advisor for SLICS

Randy Ruiz
Computer Network Specialist,
Parent Volunteer Coordinator
for SLICS

* This case is hypothetical. Any resemblance between the ficticious persons, facts, and circumstances described in this mock trial and real persons, facts, and circumstances is coincidental. It is stipulated that any enactment of this case is conducted after the named dates in the fact pattern and witness statements.

STIPULATIONS

1) The only technical information eligible for use at trial is that supplied within this packet. Other technical information or computer jargon is not allowed at trial.

2) No computers, purporting to show the actual workings of the Internet, or actual webpages, may be used at trial.

3) All names are gender non-specific and witnesses may be portrayed by either gender.

4) Witness statements are sworn and notarized.

5) All items of evidence are eligible for use at trial, following proper procedure for identification and submission. No other physical evidence, aside from those provided, can be introduced at trial.

6) All applicable motions have been made and decided. The constitutionality of all statements is not in question. All other evidentiary questions are preserved for the Court. The case is ready for trial before the Criminal Division of the Supreme Court of the State of New York.

AFFIDAVIT OF CHRIS DEAN

Witness for the Prosecution

My name is Dr. Chris Dean and I am the principal of Silas Cone High School in East Bay, New York. I've been at the school for ten years; four as vice principal and the past six as principal. Over the years, I've dealt with hundreds of instances involving student discipline, and dozens which led to criminal charges against students. Obviously, this sort of computer crime is new territory for most administrators. Our district has been dedicated to challenging students to learn how to use computer technology and gives many students the chance to have hands-on experience with creating and maintaining computer networks. Mickey Jackson's irresponsible actions damaged the trust and confidence which we had placed in SLICS and threatened school safety.

The unfortunate dark side of student access to the Internet is that parents and schools no longer have their traditional ability to control student encounters with inappropriate information. I've heard some otherwise smart people talk as if the advent of the Internet and web were only positive, letting people communicate instantly and widely, and supposedly improving knowledge. But the fact is that adults have always screened information itself and contacts with potentially dangerous individuals. The fact that the control adults had is now greatly diminished—that parental decisions on in-house magazines and television, librarians sifting of appropriate books has been made largely irrelevant by the Internet—and that is not a good thing. As an administrator responsible for maintaining order, providing a safe learning environment, and helping students meet higher standards, my job has been made much harder. Otherwise good kids may be seduced by hate sites, learn how to build bombs off the web, or become acquainted with dangerous web friends. We have a duty to limit those dangers as much as possible and to keep our schools safe.

That's why, this past spring, we urged the board to reconsider its decision to relax the application of the uniform Internet filter, instead allowing individual teachers to set classroom filters via each machine. I thought the new system would allow too much room for access to inappropriate materials, and thus increase the dangers we faced as a school. As a member of the technology committee created by the board, I argued forcefully for a remedy and was relieved when the "buffer" computer was agreed on. Having a constant record of all Internet use was the only responsible thing we could do. To do less would be to ignore proven dangers and invite trouble or disaster. The committee considered whether we needed to publicly announce the change, but after reviewing our AUP—which made it absolutely clear that the district could monitor web use and discipline inappropriate behavior—we felt that no notice was necessary. Obviously, we also thought that installing the proxy server quietly might make it more effective as a safety check on student usage. Let me make clear that when Val Watson told me about the complaints about how the Internet was functioning and asked if any changes had been made that might cause that, I answered "no" honestly. I did not realize that our new equipment had been, or could be, set to interfere with gaining access to web pages. I'm not a computer whiz myself, and knew that the technology committee had not discussed any other changes.

I was naturally upset on a number of levels when, on September 24, I became aware that Mickey Jackson had accessed and downloaded the record of my own Internet activity. The reports from teachers made it clear that school e-mail list-serves had been used to advertise Jackson's articles, that some students were refusing to participate in Internet assignments, and that I was being held up to ridicule. I was concerned that our computer system had been compromised and misused, and had no confidence that we were still recording usage or that the past month's records were secure. I was certain that Jackson's unauthorized access to the private usage records could not have been accomplished without an abuse of our AUP and perhaps breaking state laws.

Hence my quick calling of A. J. Gates, to my office. Gates claimed that Jackson had been very upset upon discovering the buffer computer and usage records, but said that they had done nothing improper. A. J. admitted that Speed had changed some settings, and that the e-mail was sent by Gates. I warned Gates not to tell anyone about our conversation, because A. J. could easily be suspended for the part played in these events.

My call to Terry Wagner resulted in Pat Chang's inspection of the computer system on Monday, September 27. Once Chang told me that settings had been changed, files deleted, and that no record of usage was being kept—all of which Chang said were potentially criminal acts if unauthorized, I immediately called the police. My experience supports not getting in the way of what should be police matters once you believe that laws have been broken.

I was not out to "get even" with Mickey Jackson for the article about me. The truth is that I sometimes collect information off the Internet, usually after hours, to use in the senior high Sunday school class I teach, centered on major problems that adults face. Hence, my visits to AA, bankruptcy, mid-life crisis, and other sites were for that purpose—Jackson's interpretation of that private data got everything wrong.

Chris Dean 11/8/99

Chris Dean, Ed.D., November 8, 1999

AFFIDAVIT OF PAT CHANG

Witness for the Prosecution

My name is Pat Chang and I am a senior technician with the computer network firm, D.R.I. We were contacted in June of 1999 by Terry Wagner, the business manager at East Bay School District, and asked to put together a proposal that would track Internet usage. That was a fairly simple thing to do; we proposed a proxy server, often called a buffer computer, that could reliably keep those records and also stores visited websites in its cache folder. Our bid was later accepted for the work and I personally installed the new system in August, which included resetting every computer in the building to recognize the proxy server.

Now before I go on, I just want to point out that this computer lingo sometimes confuses people, when much of it is really pretty simple. The proxy server I installed was just a fast computer with lots of memory and it worked just like a computer in a telephone switching system. When someone in the school clicked on a new link or sent a search request, my proxy server took that information—which all gets translated into numbers—and broadcast it onto the Internet. When another computer on the Internet gets the message that someone wants a file it has, it sends it back. When it arrives at my proxy server, the proxy checks to see which computer in the building asked for the packet, and sends it directly to that computer. All of this happens in seconds, and to most people it seems like magic or some high tech stuff that not many can understand. But actually its not all that complicated and, while amazing, its not brain surgery.

I set the system up to standard specifications, meaning that the proxy would look to its own record of sites visited in the past 12 hours before going out to the Internet to grab the needed information. The district had not requested any special security set-up, so the proxy was set to be accessed using the same system administrator's password that worked for the rest of their computer intranet. I did not know until I spoke with Dr. Dean on September 27th, that the school had a large number of students who knew that password and worked on their system. If I had been made aware of that fact, I would have created a unique password to protect the settings and the usage records on the proxy server.

When Terry Wagner called on September 24, I was out of the office at a seminar but returned the call that afternoon. While Wagner had outlined the problem in a general way, Dr. Dean detailed the downloading of the usage records and the belief that some of the settings had been changed by two students. I expressed disgust that students had broken into the system, only to learn that their initial actions had been as a result of being given the job by a teacher. I have to admit remaining a bit confused—and surprised—at the role that the student group played at the district, but turned my attention to inspecting the system.

As you can see from the log report that I printed off the proxy server, it was very clear that someone had changed the default settings on the proxy, from a 12-hour to a 30-minute setting. What this meant was that the proxy only kept a cache record of web activity for 30 minutes, before deleting those files. Thus the district's computers were going directly out to the Internet much more often that I had originally intended. Much more troubling was the fact that the usage records for

September had been deleted and the records "delete contents" setting had been reset so as to not maintain new files. If you look at the log report, you can see that the size of the usage records increased each day by about 200-300 kilobytes until September 24, when the disk space used went down to zero with the deletion of all the records. Thus the reason for having this proxy server installed had been undermined.

I think that it's clear that Mickey Jackson overstepped school and legal boundaries in going beyond what was authorized. Accessing and printing out the user records was computer trespass and deleting those user files was definitely computer tampering, even if Jackson had limited authorization to be on the system originally. No responsible teacher would expect that Jackson would go so far beyond the mandate to find the source of the seeming problem with Internet access. I am not just speculating about Jackson's role. Every computer has an individual identification number, known as the media access control number—called the MAC address in computer lingo. This is like the vehicle I.D. number that every car has or like a single fingerprint; each one is unique. On a computer network, those addresses are vital. When any computer in the school communicates with another computer, they use that MAC address which serves to funnel the communications to the right machines. We also use that MAC address to limit how many machines can directly access the network's systems software. At Silas Cone, there are ten computers whose MAC addresses are registered in the security settings. Anyone trying to make changes from any other machine is immediately denied access.

In practice it also allows us computer technicians to track what computer was used to make which changes on the system. So when Speed deleted those files, Jackson's computer left its MAC address for me to find. So I can say with absolute certainty that the deletions were made from the new computer, that is located in the back room of Val Watson's computer lab, during the morning of September 24. Its the second machine on the right as you enter the room. Finally, the system also records passwords used to access machines and access the network system. Speed Jackson's password was the only one recorded for that machine on September 24.

I hate to see a smart kid like Jackson in this kind of trouble, especially because I don't think either teenagers or adults have much of an idea of how relatively easy it is to break the law when it comes to computers and the Internet. This is a tough way to learn.

Pat Chang, 11/10/99
Pat Chang, November 10, 1999

AFFIDAVIT OF A. J. GATES

Witness for the Prosecution

My names is A. J. Gates and I'm a fifteen-year old sophomore at Silas Cone High School. I live with my parents at 86 Riverview Avenue in East Bay. I hope to pursue a career in computer chip engineering and dream of going to MIT or Cal Tech.

I was proud to be part of the school's technology crew, SLICS, and excited when Speed Jackson asked me to help find the cause of the Internet problems. Speed got that nickname by being the best at everything we did for the school—Speed did it faster and better than anyone else. It was a big deal to get asked to help Speed with anything.

We started the search on September 20th by checking out how computers in a number of classrooms performed with Internet requests. It was obvious that something odd was happening when several of the bookmarked sites gave us back outdated web pages—some up to 7 hours old. We looked to see if any of the individual settings on the machines were incorrect, but could find nothing that explained the phenomena. Speed and I both had to leave at 3:15 p.m. that day and Speed said that an early morning check would be our next step. By the time I got to school at 7:15 the next morning, Speed had already retraced our steps of the day before, with perfect "on-time" results. Speed said we'd meet again at 2:00 p.m. in Val Watson's computer lab.

That afternoon, a Tuesday, we used our system's administrator's password to access the secured part of the computer network. When we opened up the Internet browser, it became clear that a proxy server had been installed. When we checked the proxy's settings, we immediately found the source of the responses that Internet users were getting—the machine had been set to look at it's own records prior to going onto the Internet to a new web page.

Speed was very upset with the discovery and was hotly exclaiming things like "those lying bureaucrats" and "what incompetent idiots." I had never seen Speed angry before, though I had seen M. J. so enthralled with an idea or a cause that Speed was literally bouncing around a room. Speed's agitation only heightened as we looked more closely at the server's hard drive, which revealed a "User History" folder, which Speed opened and then, when we opened the daily log for September 20, gasped at. This had thousands of entries and we recognized the set-up as including the school's assigned personal identification numbers and individual computer identification numbers.

Speed said "I can't believe they would do this! They're keeping track of every Internet request!" I asked if they shouldn't have told everyone first—to which Speed didn't respond. Speed then said that we needed to print out some of the log to show Val Watson and Randy Ruiz. I was getting nervous and said that "maybe we should just close down and tell them about it," but Speed had already hit print. Speed was really steamed and said, "Don't lose your cool—we're just doing the job we were given." But by that point I was afraid that we were seeing things which no students were supposed to see or even know about. Speed then bounced back to the default settings and reset the delete time on the cache from 12 hours down to 30 minutes. Speed commented that "at least we can fix the problem that teachers knew about."

Speed and I met with Val Watson the next morning, September 22, and Speed detailed our discoveries, giving Watson the print-out from the user history folder. Watson said the next step was to talk to Randy Ruiz about this and then take it up with the school administration. Watson warned us to keep this quiet and not go back into the proxy server until things were clarified.

On Thursday the 23rd, I ran into Speed in the library. Speed told me to "take a look at this" and clicked in a search for Speed's own home webpage. I read a really convincing essay Speed wrote about the school's actions and users' privacy expectations and rights and then another short piece that lampooned Dr. Dean. I said that "You've really got some talent for getting to the bottom line. I'd bet the administration will love you even more once they see this." Speed replied that the homepage only got a few hits, from friends, and that "it would take more than words to get the school's attention."

Later in the day, I probably made the situation worse by sending an e-mail from home, via my four main classes' listserves, telling people to take a look at Speed's "bodacious postings." I wasn't trying to get Speed or myself in trouble, but I think I acted too fast and thought too little.

The next morning, Friday, September 24, my parents dropped me off early at school. I decided to go up to the computer lab to get some work done and was surprised to see Speed Jackson at a computer in the back room off the computer lab. When I opened the computer lab door, Speed seemed startled and asked loudly what I was doing in so early. Joking, I yelled back that "I wanted to fill up as much of the user history cache as possible to show how hard I was working." I then asked Speed "How about you?", while I made my way toward the back room. Speed said that I was too late—his latest research had probably used up all the server's memory. Speed was sitting at the second computer on the right, one of the two that can be used to gain access to the network's system software. Speed said "its all yours" and turned over the computer to me. I finished typing an English paper, which is what I was doing when Val Watson arrived.

I was shocked later on that Friday morning when the whole school seemed to be focused on my e-mail and Speed's homepage warnings about the school's duplicity. I'm not used to getting much attention, and this was definitely an overload. So I was already overwhelmed when my fifth period teacher, Miss Flanders, handed me a note to go see Dr. Dean immediately. I figured I was in real trouble—usually kids get called in to see the vice principal, Mr. Martinez.

Dr. Dean told me to be perfectly honest or face "dire consequences," and tell exactly what Speed and I had done. The principal was clearly angry and at one point said "so you broke into the secure Internet server" which I immediately denied. I said that Speed had reset the one default setting to allow direct access to the Internet. When Dean asked if we had disrupted the recording features, I said I didn't think so, but that Speed was very agitated and was moving very quickly.

Dr. Dean finished by yelling at me for sending the e-mail about Speed's site, saying I had violated the AUP, and that "I had better be completely forthcoming." At that point, I got this almost indescribable feeling, a fear of what I didn't know for sure, and I think I turned bright red. Dr. Dean asked "What is it? What are you remembering?" I then recounted how I found Speed in the computer lab that morning at 7:00 a.m. and how startled Speed was when I came in. I said that I hadn't done anything wrong—and hoped that the same was still true for Speed.

After Speed was arrested and Officer Vasquez interviewed me at home, and detailed how the user records and recording feature had been deleted and disabled on September 24, I had the terrible feeling that Speed really had been doing those things when I arrived on that Friday morning. At that point, I became determined to just tell the whole story and stop worrying about Speed—after all if Speed's reckless actions landed someone in jail, they had also already put me and my future in harm's way.

A.J. Gates 11/10/99

A. J. Gates, November 10, 1999

AFFIDAVIT OF MICKEY JACKSON

Witness for the Defense

My name is Mickey Jackson and I'm an eighteen-year old senior at Silas Cone High School. I live with my parents; my father is an airline pilot, and retired naval aviator. I had a Congressional appointment to the Naval Academy which Dr. Dean's vengeance has now put in jeopardy.

On a number of issues, such as the Internet filter settings in the winter and spring of 1999, I've spoken up and really gotten under the administration's skin. Members of SLICS wrote letters to the school board and local media and even led a "low tech" retro protest at a school concert—I mean imagine doing something so "sixtyish" as marching and carrying a cardboard protest sign with "Free the Filters" and "Filter Coffee Not Thought." Me and my closest SLICS friends did those things, and helped get the board to change its position—and were threatened for doing so.

I think Dr. Dean saw my Internet article in mid-September, criticizing the district for re-appropriating money to some "other computing needs" as a direct threat to the principal's new proxy server that was secretly recording all Internet usage. Dean is trying to stifle dissent and frighten other students into not posting critical articles on their own home pages by throwing me to the cops.

I know I didn't do anything criminal in pursuing Val Watson's directive. Val Watson is a wonderful teacher, who has shared a great knowledge of computers along with the broader perspective of how they should be used. We've been taught and teach about the free speech, privacy, and criminal issues arising out of computers and Internet use. Software piracy, vendors collecting and selling your personal web history and habits, successful police investigations into computer crime, Val Watson has taught them all. Before Val came to East Bay five years ago, the computers we had were boat anchors—obsolete and most useful at the and of a rope in deep water. Val has taught us to respect what computers can do well and to protect ourselves from the many dangers that computers and the Internet can bring you in contact with. I would never dishonor Val Watson by committing a computer crime.

Val Watson directly gave me the job of looking into what was up with the Internet glitch. Remember, it was no small issue—teachers and students had been frustrated just last year about the universal filter restricting access; now after winning that battle, they still couldn't get to the right pages at the right time. I tapped A. J. because Gates is a quick study and set off to do exactly what we were supposed to do. Find and fix the problem.

Our troubleshooting the problem by recreating or retracing our clients steps is standard stuff and we saw exactly what they had been reporting. The second afternoon, the 21st, when A. J. and I used our system administrator's code to access the system's settings, we were absolutely doing so with authorization. A. J. is right on one thing—I was surprised and then angry when we found the proxy server and its "user history" folder. I then knew that the district had by-passed Val Watson and SLICS and fundamentally altered policy—without any public discussion or notice to users. I don't dispute that a district can record everyone's every move, but users should be explicitly told if that's the policy. Worse, any idiot would know that those kinds of records need to be completely secure. Instead, the district had left that information readily accessible to dozens and dozens of students and adults, everyone who had any administrative rights on the computer system. That basic disregard for privacy was incompetent and at odds with everything that the district's students had been taught through Val Watson, SLICS, and its many adult volunteers.

In printing out ten pages of usage records, I was only getting a hard copy to get to Val Watson and Randy Ruiz. At that time, I knew I would help fight this battle, but had no intent or notion of using those records myself.

That night, it hit me that one way of bringing home the point of why this was so wrong was to make it personal, to show Dr. Dean a little bit of the cost of collecting private information in an unsecure system. Note that I never even mentioned the principal by name—but Dean still felt violated by having web activity thought to be private, revealed. It was meant to be a wake-up call.

So my printing out of that cache log was authorized. On the other charges that I deleted use records and disabled the recording feature—those are plain wrong. Yes, I was in the computer lab at 6:45 a.m. and surprised when A. J. showed up at 7:00, but only because no one ever comes in until 7:15 or so. I come in early a lot of days, and do my work or SLICS jobs. I gave up my seat to A. J. because I was finished with my research. Obviously I forgot to log out, which was sloppy—but at that point I had no idea that I shouldn't trust A. J. or that A. J. would be testifying against me.

I had nothing to hide from in those user logs, nothing to be afraid of. I think that maybe someone else did— and dozens of people could access that same proxy server and its settings. Remember, I thought the school was wrong as a matter of policy, that they were going to be embarrassed when proof of their new system, its recording of Internet use, and its semi-public storage of those files became public. Why would I want to destroy evidence of their incompetence? If Dr. Dean had spoken to me and Val Watson before calling the cops, this wrongful prosecution would have been avoided. But Dr. Dean wanted to show me up and scare other kids. Well, Dean may have sacred A. J. Gates, but it won't keep me quiet.

Mickey Jackson 11/12/99
Mickey Jackson, November 12, 1999

AFFIDAVIT OF VAL WATSON
Witness for the Defense

My name is Val Watson and I'm the computer science and technology coordinator at Silas Cone High School in East Bay, where I've worked since 1994. I've worked very hard to build community support and staff and student ownership of new technological applications to help young people become the masters of our new computer-driven society. SLICS and its great empowerment of students has been my proudest achievement.

The fact that I'm being asked to testify in a case involving my district and one of my brightest students on issues that should have been openly debated and settled by informed consensus, well it just seems unreal. I always try to deal openly and honestly with all comers and work toward mutually beneficial solutions to problems. My district unnecessarily created this situation by its failing to be open and communicate its policy change regarding the Internet, either to faculty, students, or the community. Perhaps its true that our AUP's wording was all inclusive enough to give the district the right to record usage, but it was still a basic change in practice and it should have been announced.

I directly authorized everything that Mickey "Speed" Jackson did on our system. I gave Speed a problem and expected Speed to get to the bottom of it, including fixing whatever glitch was found. Unfortunately, by cutting me out of the loop on the decision to install the proxy server—and with me the community experts I've engaged—Dr. Dean couldn't even give an accurate answer when I asked about Internet changes, because the principal didn't fully understand them. I find it unconscionable that Dr. Dean would resort to calling the police over a matter that Dean's own ignorance directly contributed to. If I had known that a proxy server was online, and recording all Internet usage, I never would have sent students onto that system.

I fully approve of the appropriate change that Mickey made to the proxy server's cache default setting, which alleviated the problem which was frustrating teachers. I do not believe that Mickey deleted data or disabled the usage recording function of the proxy server. The fact that those two changes were set to begin on the 24th doesn't mean they were initiated on that day. Anyone with access privileges could have intentionally made those changes anytime before that, or unintentionally, could have easily deleted the files, if unfamiliar with the system. The fact that A. J. saw Speed in my computer lab early on the 24th is meaningless—half the time Speed has been there and started a pot of coffee before I arrive at 7:20 a.m. I should explain how that lab was set up. With the growth of popularity of our computer classes, we expanded classroom computer space by setting up three machines along the front, glassed-in wall of my office, facing the front of the classroom. Two of those machines were set up to allow access to the network's system management software and were often used by SLICS students, or myself, in fixing systems problems. Naturally the computers in the backroom were considered the best seats, so I used them as a reward for excellent effort, great grades, or even an especially good answer in class. I usually keep the back room locked when I go home for the night, because it also serves as my office, with my desk and files.

However, I had given Mickey Jackson a key because Mickey came in early or stayed late so often.

So on September 24, from 7:40 a.m. to noon, there were six different classes in that computer lab—three that I taught, one taught by a colleague, and two periods of 42 minutes each where the room was open to students with study halls. The latter two were proctored by pairs of SLICS students, to provide technical assistance, and a teacher's aid to handle discipline. As few as six or as many as ten or twenty different students sat at that computer station that morning—in fact A. J. was a proctor for fourth period that day. During fourth period, at about 10:05, I stopped into my office to grab some paperwork. There were six kids working on those three computers at that point. I was in and out in a minute.

One last thing. Five years ago the thought of students managing our computer system was a radical idea. In order to satisfy the school board that the system wouldn't be abused, we limited the number of computers which could access the system management software and additionally installed a double password system to gain access to restricted areas. When a computer was started, you had to type in your five letter password to be able to use the machine at all. Then a SLICS member would also have to enter the system administrator's password—which was changed each year to help prevent hacking. Unfortunately the system wasn't perfect, because we discouraged students from turning off computers during the day. So whoever was first on the computer opened the door, so to speak, to everyone who followed if they forgot to log out. The fact that Speed's password opened the door to the machine which was used to delete data doesn't prove that Speed was the one doing the deleting—it only proves that Speed did not log out that morning. A bunch of other kids also used that machine, including A. J., who was sittting at it when I arrived at 7:20 on Friday the 24th.

We teach all our students to assume that their every move is being recorded when they are on the Internet. My students know that if there is a way to make money off collecting and bundling private information on the Internet, then it is being done. The district's lack of knowledge and communication allowed their vendor, D.R.I., to install a powerful proxy server with inadequate security to protect its sensitive records. We are lucky that no one collected and sold that user information, straight off our own system.

Mickey Jackson is one of the finest young people I have ever met. Mickey's intellect and dedication is matched by personal honesty and commitment to making a positive contribution to the community. That our district's lack of vision and distrust of its own students and staff created this situation is clear. To have Mickey Jackson's career and life short-circuited because of the district's failures would be tragic.

Val Watson, 11/12/99

Val Watson, November 12, 1999

AFFIDAVIT OF RANDY RUIZ
Witness for the Defense

My name is Randy Ruiz and I live at 400 Granite Drive in East Bay, NY. I work for the major producer and installer of Internet router systems in the world, where I am a senior engineer. I also serve as the chair of the community board of directors assisting SLICS. I personally know, respect, and admire both Val Watson and Speed Jackson.

I think that, as a society, we are having trouble coming to grips with many of the computer and Internet-driven changes facing us. As a result, while we pass laws attempting to regulate and thwart inappropriate computer behavior, we have a hard time knowing when and where they should be applied. I have given legislative and courtroom testimony on these issues and have repeatedly warned of the need to be explicit in language and careful in application of legal sanctions. I think that Dr. Dean and the police were overly anxious to make an example of this fine young person.

Without doubt, Speed's initial entrance to the computer and to the secure part of the system, were authorized by Val Watson. Speed's change of the default setting to allow direct access to the Internet was also proper, as was the printout of the user log. That allowed Val Watson to fax me a copy of that information on September 22, to gain my reaction and advice. From my examination of the proxy server log report showing when changes were implemented on the proxy server, I can't conclude that we know who made the deletions of records or disabled the recording function. I think that Dr. Dean jumped to an unfounded conclusion, assuming that Speed's actions were not authorized and improperly called the police.

Speed may have been ill-advised in looking at and acting on information from the printout of the user log, but that doesn't mean Speed was unauthorized when it was being printed out. Speed's claim that it was meant for Val and myself match the actions taken—it was passed on to Val at the next possible time, the morning of September 22.

As an expert in hooking companies up to the Internet, dealing with all facets of technical e-commerce issues, I still never lose sight of the fact that I need to fully understand how a client does business, before I turn to wiring in a solution. The district and D.R.I. failed miserably in that vital process of communicating. The district didn't raise privacy concerns and D.R.I. was kept ignorant of the dozens of users who, uniquely, had access to system administrators' privileges. Thus, they did business, but failed to do it well.

I think that the sloppy thinking that got us into this mess is continuing with the conclusions being drawn by the prosecution's witnesses. We shouldn't let the technical nature of this case obscure the need for real, solid, indisputable evidence of wrongdoing. The access and trespass charges are bogus. The tampering charge lacks one important element of proof—evidence that only Speed might have made those deletions.

I've spent dozens of hours helping to wire classrooms and network machines at Silas Cone, and took the lead in designing the secure system that protects students' records, but gives administrators and teachers appropriate access. Those Internet use records should have been treated with the same care. I am appalled that this sloppiness happened in my own district. If anyone should be punished, its those responsible for bringing this situation about, not the innocent and properly indignant student who discovered the district's flawed Internet set-up.

Randy Ruiz 11/15/99

Randy Ruiz, November 15, 1999

EAST BAY SCHOOL DISTRICT

COMPUTER NETWORK USER GUIDELINES

Student and Parent Permission Form

Your child has requested access to the East Bay School District Computer Network. This access includes connections to computers through the Internet, which would connect your child with educational resources all over the world. In accepting an account, your child accepts the responsibility of using the network in an appropriate manner. It is important that you understand his/her responsibilities as well.

Please read with your child the East Bay School District Board of Education's *Acceptable Use of Computer Networks Policy 5.1,* and the *Computer Network User Guidelines.* After reading, please complete this form to indicate that you agree to the terms and conditions outlined. The signatures of **both** the student and parent/guardian, indicating that you have read and agreed to our *Use and Guidelines,* are mandatory before access may be granted to the EBSD network.

Please complete this form and return it to your child's school.

As a user of the East Bay School District Computer Network, I have read and agree to comply with the *Computer Network User Guidelines.*

Student Signature: Mickey Jackson

Student Name (Please Print): MICKEY JACKSON

Date: 9/9/99

Student's School: Silas Cove

Grade: 12

As parent/legal guardian of the student signing above, I grant permission for my child to access networked computer services such as electronic mail and the Internet. I have read and agree to the **EBSD** *Computer Network User Guidelines.* I understand that some materials on the Internet are objectionable; therefore I agree to accept responsibility for guiding my child, and conveying to her/him appropriate standards for selecting, sharing and/or exploring Internet resources.

Parent/Guardian Signature: Ann Jackson

Parent/Guardian Name (Please Print): ANN JACKSON

Date: 9/8/99

Address: 32 MARBLE TER
EAST BAY, NY

Home Telephone: 567-1380

Daytime Telephone: SAME

If you have any questions or concerns, please contact
Val Watson, EBSD Director of Technology Education, at 837-4100 ext. 432.

East Bay School District
Computer Network User Guidelines

Resources available through the District networked computers are available for use by students, staff, and the community. All users must understand and practice proper ethical use and security. Access to the network is considered a privilege, not a right. Based on the acceptable use guidelines outlined in this document, the system administrators in cooperation with District Administration may monitor or close an account at any time. All decisions of District Administration are final.

East Bay School District **does not have control of the information on the Internet.** Some sites accessible via the Internet contain material that is inappropriate for educational use in a K-12 school setting. The District does not condone the use of such materials and will not permit usage of such in the school environment. The District is not responsible for the accuracy or quality of information obtained through its Internet accounts.

Acceptable Uses:

1. Use consistent with the mission of the East Bay School District.
2. Use that encourages efficient, cooperative, and creative methods to perform the user's job duties or educational tasks.
3. Use in support of research and education consistent with State Learning Standards.
4. To provide unique resources and collaborative projects.
5. Authorized uses by student members of SLICS in support of District Technology needs.

Unacceptable Uses:

1. Use of school technology resources for a commercial, political, or profit-making enterprise.
2. Accessing or distributing inappropriate material or any material specifically prohibited by federal, state or local laws.
3. Attempts to illegally access or alter files, data, or accounts. Students and staff must limit their activity to those areas of use made available to them.
4. Activities which interfere with student and staff access to network resources.
5. Accessing (or attempting to access) network accounts not assigned to you.
6. Sharing your password or account access with others.
7. Giving out personal information such as home address or telephone number.
8. Deliberately or intentionally damaging hardware or software.

Board of Education Policy 5.1:

Acceptable Use of Computer Networks

The Board of Education of the East Bay School District recognizes that the main purpose for the use of district computers is to support learning and enhance instruction.

To this end the Board supports a strong computer science and Technology Education program, the innovative work of SLICS and the continued access by students to educationally valid information resources along with the development by staff of appropriate skills to analyze, evaluate, and use such resources.

The Board expects that staff will integrate use of such resources throughout the curriculum and that staff will provide guidance and instruction to students in the appropriate use of such resources.

Students are responsible for good behavior on school computer networks just as they are in all school activities. Access to network services will be provided to students who act in a responsible manner. Students found in violation of these policies may have their network privileges revoked, may be suspended or expelled, or may face legal action, in keeping with the severity of the violation.

- *Adopted August 15, 1996*

www.speedsworld.hypocrisy

Hypocrisy.org and Incompetence.com

After gaining a well-deserved statewide reputation for its coherent and effective computer technology education program and its innovative inclusion of the community and students in building an effective program, the East Bay School District and Silas Cone High School have given shame and hypocrisy a new home. Only months after the culmination of a well-reasoned public debate over suitable filter systems for the Internet, my district has secretly installed a new proxy server, set to record all Internet usage, and done so with no notice to parents, students, or staff. Worse, this was done with no regard to the legitimate privacy rights of users, as the usage history folder was left almost in the open, easily accessible to any one of dozens of individuals.

Students, stand up for what's right! Tell your parents and the school board that you want to know who botched this issue and this set-up. Give us Respect! Give us our money back!

www.speedsworld.guess

GUESS WHO'S GOING WHERE?

What high school administrator is frustrated, stressed, and thinking of making major changes in their life?

SOMEONE is spending an awful lot of time on the web, surfing for advice on stress management, mid-life career changes, and seems CAUGHT between seeking help with a GAMBLING problem and PLUNGING even

deeper

into

DEBT.

Maybe THAT explains the REPEAT visits to sites offering ***bankruptcy*** advice and the often heard comment from the administrator's own lips, "NO DICE".

NOW, aren't you glad that **YOUR OWN** use records are being kept in an ***UNSECURE*** folder on our school's computer system? Where have **YOU** been lately that you want the

WHOLE WORLD

to know about?

Proxy Server Log Report

```
Name                                        Size              Last Modified

Systems Folder

  Proxy Server

    Border Manager

    Cache Statistics
    Cache Settings
              Auto delete after [ .5 ] hours                  Sept. 21,  3:00 p.m.


    Connection Statistics
         Use Records
              User History folder                             Sept. 24, 12:00 p.m.
                   Daily Log     9/9/99      150k
                   Daily Log     9/10/99     310k
                   Daily Log     9/11/99     361k
                   Daily Log     9/12/99     361k
                   Daily Log     9/13/99     513k
                   Daily Log     9/14/99     757k
                   Daily Log     9/15/99    1018k
                   Daily Log     9/16/99    1381k
                   Daily Log     9/17/99    1592k
                   Daily Log     9/18/99    1592k
                   Daily Log     9/19/99    1879k
                   Daily Log     9/20/99    2316k
                   Daily Log     9/21/99    2744k
                   Daily Log     9/22/99    3197k
                   Daily Log     9/23/99    3503k
                   Daily Log     9/24/99       0k
                   Daily Log     9/25/99       0k
                   Daily Log     9/26/99       0k
                   Daily Log     9/27/99       0k

              Delete Contents after [ 0 ] days                Sept. 24, 12:05 a.m.
```

PART VI

PERTINENT LAW AND INFORMATION

New York Consolidated Laws

§ 156.00 Penal. Offenses involving computers; definition of terms.

The following definitions are applicable to this chapter except where different meanings are expressly specified:

1. "Computer" means a device or group of devices which, by manipulation of electronic, magnetic, optical or electrochemical impulses, pursuant to a computer program, can automatically perform arithmetic, logical, storage or retrieval operations with or on computer data, and includes any connected or directly related device, equipment or facility which enables such computer to store, retrieve or communicate to or from a person, another computer or another device the results of computer operations, computer programs or computer data.

2. "Computer program" is property and means an ordered set of data representing coded instructions or statements that, when executed by computer, cause the computer to process data or direct the computer to perform one or more computer operations or both and may be in any form, including magnetic storage media, punched cards, or stored internally in the memory of the computer.

3. "Computer data" is property and means a representation of information, knowledge, facts, concepts or instructions which are being processed, or have been processed in a computer and may be in any form, including magnetic storage media, punched cards, or stored internally in the memory of the computer.

4. "Computer service" means any and all services provided by or through the facilities of any computer communication system allowing the input, output, examination, or transfer, of computer data or computer programs from one computer to another.

5. "Computer material" is property and means any computer data or computer program which:

(a) contains records of the medical history or medical treatment of an identified or readily identifiable individual or individuals. This term shall not apply to the gaining access to or duplication solely of the medical history or medical treatment records of a person by that person or by another specifically authorized by the person whose records are gained access to or duplicated; or

(b) contains records maintained by the state or any political subdivision thereof or any governmental instrumentality within the state which contains any information concerning a person, as defined in subdivision seven of section 10.00 of this chapter, which because of name, number, symbol, mark or other identifier, can be used to identify the person and which is otherwise prohibited by law from being disclosed. This term shall not apply to the gaining access to or duplication solely of records of a person by that person or by another specifically authorized by the person whose records are gained access to or duplicated; or

(c) is not and is not intended to be available to anyone other than the person or persons rightfully in possession thereof or selected persons having access thereto with his or their consent and which accords or may accord such rightful possessors an advantage over competitors or other persons who do not have knowledge or the benefit thereof.

6. “Uses a computer or computer service without authorization” means the use of a computer or computer service without the permission of, or in excess of the permission of, the owner or lessor or someone licensed or privileged by the owner or lessor after notice to that effect to the user of the computer or computer service has been given by:

(a) giving actual notice in writing or orally to the user; or

(b) prominently posting written notice adjacent to the computer being utilized by the user; or

(c) a notice that is displayed on, printed out on or announced by the computer being utilized by the user. Proof that the computer is programmed to automatically display, print or announce such notice or a notice prohibiting copying, reproduction or duplication shall be presumptive evidence that such notice was displayed, printed or announced.

7. “Felony” as used in this article means any felony defined in the laws of this state or any offense defined in the laws of any other jurisdiction for which a sentence to a term of imprisonment in excess of one year is authorized in this state.

§ 156.05 Penal. Unauthorized use of a computer.

A person is guilty of unauthorized use of a computer when he knowingly uses or causes to be used a computer or computer service without authorization and the computer utilized is equipped or programmed with any device or coding system, a function of which is to prevent the unauthorized use of said computer or computer system.

Unauthorized use of a computer is a class A misdemeanor.

§ 156.10 Penal. Computer trespass.

A person is guilty of computer trespass when he knowingly uses or causes to be used a computer or computer service without authorization and:

1. he does so with an intent to commit or attempt to commit or further the commission of any felony; or

2. he thereby knowingly gains access to computer material.

Computer trespass is a class E felony.

§ 156.20 Penal. Computer tampering in the fourth degree.

A person is guilty of computer tampering in the fourth degree when he uses or causes to be used a computer or computer service and having no right to do so he intentionally alters in any manner or destroys computer data or a computer program of another person.

Computer tampering in the fourth degree is a class A misdemeanor.

RELATED CASES

People v. O'Grady, A.D. Third Dept. Slip Opinion 695 NYS2d 140 (July 1999) — § 156.10. A woman walked into a bank and accosted one of its employees, saying, "Stay away from my husband!" It turned out that she was the employee's boyfriend's estranged spouse, whose sister worked at NY State Department of Taxation and Finance. That Dept.'s Inspector General learned, following investigation, that the defendant (spouse's sister) had accessed records on the bank employee's family without authorization, despite fact that family members had no outstanding tax issues at the time. Her log-in and employee ID were used to gain access. Records also showed that Defendant was working on the day in question. Held: Conviction for four counts of computer trespass AFFIRMED; ".... foregoing proof not only amply justifies the jury's inference that defendant was the individual who had unlawfully accessed the Department's computer records but, further, excludes to a moral certainty any possible hypothesis of innocence."

People v. Versaggi, 83 N.Y.2d 123, 608 N.Y.S.2d 155 (1994) Defendant convicted of two counts of computer tampering in the second degree under Penal Law § 156.20 for altering two computer programs designed to provide uninterrupted phone service to the Eastman Kodak Corporation. Defendant, a computer technician, was employed to maintain and oversee a different system. Co-employees testified that defendant issued commands to cause the Eastman Kodak program to shut down completely as he bypassed a security system designed to protect the program. By disconnecting the program and causing the computer to shut down he altered the program in some manner. "Whether the defendant used existing instructions to direct the phone system off-line or input new instructions accomplishing the same thing is legally irrelevant. He made the system 'different in some particular characteristic without changing [it] to something else....' The intended purpose of the computer program was sabotaged. Conviction affirmed."

People v. Lett, 187 A.D.2d 456, 589 NYS2d 528 (1992) Appeal of conviction for computer trespass AFFIRMED because Defendant's accomplice was observed entering overtime for Defendant into a computer terminal on three separate occasions. Entries that were verified by certain computer records but unsupported by sign-in sheets or other authenticating documentation are consistent with a conclusion of guilt.

People v. Angeles, 180 M. 2d 146 (March 1999) — § 156.05. Where defendant was charged with selling a customer list for money, the court decided there can be no unauthorized use of computer unless the computer has a device to prevent unauthorized use. Examining legislative history for the unauthorized use section, the Court opines: "The Legislature thus put computer owners on notice that in order to receive the protection of the criminal statute, they must equip their computers with some kind of protection mechanism, such as a password requirement or a lock... In the present case, to assume the existence of such a system would be pure conjecture. The mere allegation that an individual has obtained access to a computer without the owner's authority is insufficient to plead a violation of Penal Law § 156.05. This count of the information is therefore dismissed." Court also distinguishes §§ 156.30 and 156.35.

People v. Katakam, 172 Misc.2d 943 (1997) §§ 156.10, 156.30, 156.35. computer consultant left the employ of Goldman Sachs to take position with J.P. Morgan. At Goldman Sachs, he had authorized access to computer directories with utility files and script files. He put the script libraries in his personal file and two weeks after departing, had a colleague e-mail them to him at new job. Held: criminal liability under § 156.30(1) is predicated solely upon his duplication of the files, not whether they held commercial value for any other company. Testimony of Goldman Sachs V.P. established that Defendant had no right to possess these programs. But no culpability under either of two subsections of computer trespass statute, § 156.10, because there was no proof that he used the Goldman Sachs computers without authorization. Accessing, and even duplicating certain files, constituted neither a personal nor non business use nor disclosure to an outsider. His "actions do not smack of computer trespass." Since he was not acting in excess of authorization when he accessed these files, those counts were dismissed.

* * * * *

The following case is of interest because this year's Interstate Tournament is being conducted with Maryland. However, this case should not be used in the statewide tournament because it does not have the same standing as New York cases interpreting New York statutes.

Terry Dewain Briggs v. State of Maryland 348 Md.470, 704 A.2D 904 (1998).

Defendant Briggs, a computer programmer, was convicted of unauthorized access to computers in violation of Maryland Law Article 27 § 146 (c) (2).

Testimony adduced at trial showed Briggs was entrusted the management of entire computer system by his employer, which job required him to enter passwords in the system. Briggs placed passwords into separate file two days before resigning his position due to a contract dispute and refused to disclose it after his resignation. Briggs was sued civilly and charged separately with theft of computers and unauthorized access to computers. The jury acquitted Briggs of the theft charge.

In reversing the conviction, the Maryland Court of Appeals held that in order to sustain a conviction the State had to prove (1) that Briggs intentionally and willfully accessed a computer or computer system; (2) that the access was without authorization; and (3) the access was with the intent to interrupt the operation of the computer system. In failing to prove that the access was "without authorization" the second element of this three pronged test was not satisfied. Accordingly the State did not prove that Briggs' conduct came within the prohibition of the statute.