



9-1-1986

Piracy, Privacy, and Security: Legal Issues of Computer Use in Schools

Grover H. Baldwin
Indiana State University

Follow this and additional works at: <https://newprairiepress.org/edconsiderations>



Part of the [Higher Education Commons](#)



This work is licensed under a [Creative Commons Attribution-Noncommercial-Share Alike 4.0 License](#).

Recommended Citation

Baldwin, Grover H. (1986) "Piracy, Privacy, and Security: Legal Issues of Computer Use in Schools," *Educational Considerations*: Vol. 13: No. 3. <https://doi.org/10.4148/0146-9282.1700>

This Article is brought to you for free and open access by New Prairie Press. It has been accepted for inclusion in Educational Considerations by an authorized administrator of New Prairie Press. For more information, please contact cads@k-state.edu.

The proliferation of microcomputer software has exacerbated three problems: piracy of software . . . piracy of information . . . and security of data. . .

Piracy, Privacy, and Security: Legal Issues of Computer Use in Schools

by Dr. Grover H. Baldwin

Since the early 1980s, there has been a proliferation of microcomputers in the schools. Fueled by the external demands for computer literacy, the rush to keep up with other nations technologically, and the "promise" of greater achievement at lesser costs, school districts have purchased microcomputers, developed curriculum, and purchased software at an amazing rate. The costs of hardware have come down and greater power is now available for less money; however, the cost of software has remained high.

Concurrently, the infusion of software programs into the schools has not been consistently well-planned across district lines. This has led to unrestricted and uncontrolled use of the software, lack of solid curriculum planning, random infusion of computers into the instructional process, and the unrestricted access to both program and data disks, and schoolwide databases, by a variety of school personnel.

This proliferation of microcomputer software has exacerbated three problems: **piracy** of software to "beat" the high cost of programs; **privacy** about information of students' lives through the use of programs not appropriate for instructional purposes and easy access to students' information; and **security** of data disks and databases via the ready access by any school employee, whether or not he has a legitimate interest in the information.

This article will examine these three legal issues involved with the use of microcomputers in the public schools

Piracy and Software Copyright Protection

In their work on intellectual property law, Kintner and Lahr (1975) made only passing reference to computers and copyrights, saying that it was an arising problem. The American Library Association handbook on copyright law failed to mention the legal issues surrounding the copyrights at-

tached to computer software (1977). Yet, one year later, the National Commission on New Technological Uses of Copyrighted Works (Final Report, 1978) dealt at great length with the additional changes needed in the copyright law to cover this growing area. These changes became part of the revised copyright law and have a dramatic effect on the school use of computer software.

With the purchase of any piece of software, the owner signs a licensing agreement. By signing the agreement, the owner of the software agrees to abide by the stipulations of that agreement. Typically, the owner is permitted to make one archival copy of the piece of software in case the original is destroyed or damaged beyond normal use. Stipulated in licensing agreements is the clause that the owner of the software "may not use, copy, modify, or transfer the program or documentation" except as provided within the licensing agreement and any unauthorized use is a copyright violation punishable by law (Microsoft, 1984).

With the high cost of software, and the decrease in school funds available to purchase additional pieces of software for any particular grade level or subject area, some school districts have made multiple copies for all the classrooms/teachers needing the program. While the piracy issue has been with us since the beginning of the "micro" revolution, and while "locksmith" programs abound to open up the program for multiple copies, the legal issues involved in such activities are just now coming to the fore.

There are two copyright issues involved here. First there is the issue of fair use. The fair use standard involves four aspects:

- (1) the purpose and character of the use, including whether such use is of a commercial nature or is for a non-profit educational purposes;
 - (2) the nature of the copyrighted work;
 - (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole, and;
 - (4) the effect of the use upon the potential market for or value of the copyrighted work.
- (17 USCA 107).

The most important aspects of the fair use doctrine for school districts are numbers 1 and 4. Schools are normally considered non-profit educational institutions. However, when they engage in the transmission of knowledge via use of multiple copies of copyrighted materials, they are in violation of the law and lose that status. The recent decisions in the Encyclopedia Britannica vs. Crooks cases bring this point poignantly home (1982; 1983). While the copied materials in this BOCES case were films, and while the materials were distributed among teachers in the BOCES service area, the U.S. District Court found the BOCES in violation of the copyright law as they had made multiple copies, and had kept them beyond the normal two-three day rental period. Under these circumstances, the Court held that the BOCES had violated their non-profit educational status. Further recognition of copyright violations, through making multiple copies of computer software, comes from the SAS Institute, Inc. vs. S & H Computer Software, Inc. decision (1985).

The second issue, that of the effect on the potential market for or value of the copyrighted work, should be obvious. By making multiple copies to permit the school district to lessen its instructional costs and save on the high cost of software, the educational agency is in direct violation of the copyright law. An offshoot of this issue is the typing of com-

Dr. Grover H. Baldwin is an associate professor in the Department of Educational Administration at Indiana State University, Terre Haute, Ind.

puter programs from magazines that carry listings of computer programs. While the court has held that the purchaser of the magazine may type in the program, and use it for his own use, the listing cannot be copied and distributed to other individuals, nor may a **third party** copy the program into an electronic device to permit operation of the program (Micro-Spart, Inc., 1984).

For computer software, making a copy includes not only copying to another disk, but the loading a program into electronic memory devices and using the program to control activities of the machines (William Electronics, Inc., 1982). Thus, subsequent booting to additional computers, even if there is only one copy of the program, or the use of the program in a networking set-up, have the potential of being a violation of the copyright law. Therefore, the only valid copies that can be made of computer programs are the single, archival copies that permit retrieval if disks are damaged or programs crash.

While many school districts, service agencies, and school personnel may be tempted to "forget" the copyright law pertinent to computer software, the penalties are rather stiff. Growing out of the Sony case (Sony Corp., 1984), the standard of contributory infringement of copyright violations was established. This notion of contributory infringement was enforced in the *Encyclopedia Britannica* decisions (1982; 1983). The contributory infringer is considered to be the individual who is "in a position to control the use of copyrighted works by others and had authorized the use without permission from the copyright owner" (Sony, at 437). Thus, this standard holds the school administrator (both district superintendents and building principals) responsible for the acts of copyright violation of their employees. The penalties range from a minimum of \$250 for infringement of any one work to a maximum of \$50,000 if the court finds willful infringement for damages against the copyright owner. Also, criminal charges and penalties may rise to \$10,000 and/or imprisonment of not more than one year for willful infringement of copyrights for commercial advantage or private financial gain. These penalties were inflicted for **each incident** of copying in the Williams case, and have dramatic effect if we consider the subsequent "booting" and networking capabilities districts are beginning to have implemented in the schools. The penalties for violation of fair use and contributory infringement far outweigh the cost of purchasing additional copies for school use.

Privacy and Security

Turning to the use of computers and software within the schools, we find the second problem area, that of privacy and security. Privacy is used here in the context of both privacy of information about the students' attitudes and beliefs, and privacy and security of information dealing with records kept by school district personnel on individual students.

Under the Hatch Amendment (20 USCA 1232h), pupils are protected from certain types of questions that tend to reveal information about their political beliefs; mental and psychological problems; sexual behavior and attitudes; illegal, anti-social, self-incriminating, and demeaning behavior; and specified other pieces of information that are potentially damaging to their health, safety, and well-being. While the amendment covers psychiatric or psychological examinations, testing, and treatment, the amendment has been used to permit parents and concerned citizens to examine the instructional materials and curricular programs of schools. The rub for microcomputer software comes with

the use of specific programs designed to assist students to be come familiar with the operation of computers. These conversational programs are designed to permit student interaction, with little fear of fouling up the computer program, while gaining an understanding of the operation of the computer and its potential. However, what about the nature of the conversational program and its suitability for specific age groups of children? Two conversational programs come to mind that create dangerous and embarrassing situations for students and school personnel. These two programs, "Hello" or "Psycho," are very entertaining, both have interactive capabilities, but both are potentially dangerous. "Hello" asks students questions about sex, money, health, or job. "Psycho" asks the student to use projective analysis to render a description of the inner personality characteristics of the individual. It ends with an explanation of the respondent's sex drive.

Yes, they are cute and the vast majority of students will be able to handle the questions in stride. However, in the context of the developing new teaching techniques and instructional methodology using microcomputers, such material is open to inspection under the Hatch Amendment. Not only can it be inspected, but the use of such programs places schools in the similar dilemma fostered by values education and moral development programs. Further, while not a psychological examination in the strict sense of the Hatch Amendment, the use of such programs as part of computer literacy programs does have the effect of holding students up to sarcasm, ridicule, and peer approval/disapproval and comes close to the burgeoning notion of psychological maltreatment. Again, while most students will deal with the program easily, the use of such programs does open the schools, and school personnel, to close scrutiny of the public under the Hatch Amendment.

An additional privacy problem, also linked to security of information, deals with information about student attitudes, values, and parental background when gathered via career and vocational guidance programs. This adds to the problem of privacy, especially if the information pertinent to these sensitive areas is retained for later use by guidance personnel, but is accessible by school personnel.

The second aspect of privacy links with security of data and databases that contain information regarding students, both personal and academic. The problem lies in who has access to this information and for what purpose. The Family Rights and Privacy Act makes provision for who has access to files and information regarding students (20 USCA 1232g). The amendment provides that access to educational records must be with parental, or student, consent except for school officials within the school district who have a legitimate educational interest, or school officials of other systems in which the student seeks to enroll. Given computer programs dealing with database management, recordkeeping, and gradekeeping, anyone accessing these files for a particular individual will be faced with a screen full of other information not pertinent to the particular query or their legitimate interest. While professional staff members, including teachers, have an interest in students they are dealing with in a particular year, and perhaps need additional family information, the computer programs used in schools allow for global access to all information by anyone using the program. Parental permission may not be necessary to access student information by school personnel, but the school must establish the limits of legitimate educational purpose and work from that position.

There is also the concern for security of the information stored on disks and internal memory of computers.

Given the recent spate of illegal intrusions into computer systems by individuals not entitled to have access to such information, extraordinary precautions need to be established. Policy must be established to determine who enters and edits data in school files; who has access to what files; who can copy information from the files; and who should have ready access to district, building, and teacher's files. Further precautions must be taken to guard against breaks in security of the information. Part of the security of building and district information flows back to the copying problem mentioned earlier.

The key to the security, privacy, and piracy issues is supervision by the building administrator and the awareness of the other school personnel to the problems they face in dealing with the use of microcomputers in the schools.

Recommendations for School Personnel: for Piracy:

1. School districts should seek software from companies that offer "site licensing." This is a relatively new phenomena and one that, while costly initially, will benefit the schools by payment of a one-time licensing fee and allowing school personnel to make multiple copies as needed. If that is not feasible, then the district should purchase one copy for each site (building or classroom) in which the program would be used.

2. In lieu of site licensing, school district and building policies need to be established and supervised covering the following area:

- a. Making of one archival copy and distribution of the software program using the single copy for use in the classroom or office.

- b. Close security by the building administrator of the use of the software to ensure that multiple copies are not made.

- c. All software should be inventoried and regularly accounted for, both in terms of its use and for possible violation of the copyright laws.

- d. Specific in-service should be held to delineate the overall copyright law and its effects on teachers and other school personnel. All school personnel must be cognizant of the law and the penalties involved for its violation.

- e. On all copyrighted material that would be used by school personnel, the Copyright Statement should be prominently displayed.

For Privacy and Security:

While most school districts have policy statements on accessibility and privacy of student records, they have been concerned with the written records stored in the schools. With the use of computerized databases, additional precautions need to be taken to insure the non-violation of the Family Rights and Privacy Act.

1. Establish exact policies and procedures for access to computerized databanks of student records, including who has access and for what purpose; checkout and return procedures; who may copy data from the master files; and empower one individual per site with oversight responsibility for these areas.

2. In hiring an individual to enter, edit, and delete data

from school records, place emphasis on the individual's capability of dealing with confidential data. While routine data entry might be handled by a paraprofessional or a volunteer parent, as they are dealing with student and family information, care must be taken to insure the confidentiality of information will be kept.

3. Make use of passwords to insure that in the event data is obtained by non-authorized school personnel, that they cannot access areas to which they are not permitted.

4. Provide teachers with data disks on which to maintain their own data files of student grades and other academic information so that this information is protected. Further, insure that teachers have a safe place, preferably locked and secure, or via password arrangements, so that their data cannot be accessed and altered.

5. See that data on student's achievement is placed on master files at the end of the year and that individual teacher records are destroyed.

6. In dealing with the curricular issues found above, establish a software evaluation process, that includes parents and students, that evaluates the proposed software not only in terms of its applicability to the curriculum and instruction process, but also protects the rights and privacy of individual students.

Overall, the use of microcomputers will continue to grow in schools. The need for additional software to fulfill teacher demands will increase. The need for access to information stored in various databases will become increasingly pronounced. Recognition of these factors, and the legal issues raised above, will force school districts to reassess their policies regarding purchase and use of such materials. While the legal issues are important, they are manageable and can lead to greater and more effective use of microcomputers in the schools.

Reference

- American Library Association. (1977). *The new copyright law*. Washington.
- Copyright, 17 USCA 101-509 (1983)
- Encyclopedia Britannica Educational Corporation v. Crooks, 542 F.Supp. 1156 (USDA, W.D. New York, 1982).
- Encyclopedia Britannica Educational Corporation v. Crooks, 558 F.Supp. 1247 (USDA, W.D. New York 1983).
- Family rights and privacy act, 20 USCA 1232g.
- . (1978). *Final report*. Washington: National Commission on New Technological Uses of Copyrighted Works.
- Kintner, E. W., and Lahr, J. L. (1975). *An intellectual property law primer*. New York: Macmillan.
- Microsoft, (1984). *Microsoft licensing agreement*. Bellevue, WA: Microsoft.
- Micro-Sparc, Inc. v. Amtype Corp., 592 F.Supp. 33 (USDC, D. Mass 1984).
- Protection of pupil rights. (Hatch Amendment). 20 USCA §1232h.
- SAS Institute, Inc. v. S & H Computer Systems, Inc., 602 F.Supp. 816 (USDC, M.D. Tenn. 1985).
- Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417 (1984).
- Williams Electronics, Inc. v. Artic International, Inc., 685 F2d 870 (3rd Cir. 1982).