## INFORMATION TO USERS

This material was produced from a microfilm copy of the original document. While the most advanced technological means to photograph and reproduce this document have been used, the quality is heavily dependent upon the quality of the original submitted.

The following explanation of techniques is provided to help you understand markings or patterns which may appear on this reproduction.

1. The sign or "target" for pages apparently lacking from the document photographed is "Missing Page(s)". If it was possible to obtain the missing page(s) or section, they are spliced into the film along with adjacent pages. This may have necessitated cutting thru an image and duplicating adjacent pages to insure you complete continuity.

2. When an image on the film is obliterated with a large round black mark, it is an indication that the photographer suspected that the copy may have moved during exposure and thus cause a blurred image. You will find a good image of the page in the adjacent frame.

3. When a map, drawing or chart, etc., was part of the material being photographed the photographer followed a definite method in "sectioning" the material. It is customary to begin photoing at the upper left hand corner of a large sheet and to continue photoing from left to right in equal sections with a small overlap. If necessary, sectioning is continued again — beginning below the first row and continuing on until complete.

4. The majority of users indicate that the textual content is of greatest value, however, a somewhat higher quality reproduction could be made from "photographs" if essential to the understanding of the dissertation. Silver prints of "photographs" may be ordered at additional charge by writing the Order Department, giving the catalog number, title, author and specific pages you wish reproduced.

5. PLEASE NOTE: Some pages may have indistinct print. Filmed as received.

**Xerox University Microfilms**

300 North Zeeb Road
Ann Arbor, Michigan 48106

75-10,364

CORASICK, Margaret John, 1942-
PROTECTION OF COMPUTER-BASED INFORMATION:
A STUDY OF THE MEANS OF PROTECTION AND THE
LEGAL FRAMEWORK IN WHICH SUCH PROTECTION
IS UNDERTAKEN.

Lehigh University, Ph.D., 1974
Information Science

**Xerox University Microfilms**, Ann Arbor, Michigan 48106

THIS DISSERTATION HAS BEEN MICROFILMED EXACTLY AS RECEIVED.

# PROTECTION OF COMPUTER-BASED INFORMATION: A STUDY OF THE MEANS OF PROTECTION AND THE LEGAL FRAMEWORK IN WHICH SUCH PROTECTION IS UNDERTAKEN

by

Margaret J. Corasick

A Dissertation

Presented to the Graduate Committee

of Lehigh University

in Candidacy for the Degree of

Doctor of Philosophy

in

Information Science

Lehigh University

1974

Approved and recommended for acceptance as a dissertation in partial fulfillment of the requirements for the degree of Doctor of Philosophy.

November 10, 1974

Professor Robert F. Barnes

Accepted 13 Dec 1974

Special committee directing the doctoral work of Ms. Margaret J. Corasick

Professor Robert F. Barnes

Dean Brian G. Brockway

Professor Donald J. Hillman

Professor Andrew J. Kasarda

## ACKNOWLEDGEMENTS

I would like to thank Professor Robert F. Barnes and Dean Brian G. Brockway for their generosity with their time, patience, and many helpful suggestions during the preparation of this dissertation. In large part, their direction has made this work possible.

CONTENTS


| | | |
|---|---|---|
| I. | Introduction | 3 |
| II. | Protection within the Computer System: The State of the Art | 13 |
| III. | Present Legal Remedies | 39 |
| IV. | The Interests at Stake | 71 |
| V. | Proposed Technical Solutions | 86 |
| VI. | Legal Solutions | 101 |
| VII. | Conclusion | 128 |

## ABSTRACT

A special case of the information security problem is protection of commercially obtained information on a general purpose data processing system. Such data is prepared for the purpose of marketing to users with conventional computing configurations,and must be protected given the present state of the art. These configurations are not amenable to increases in operating overhead or advanced design development required by protection systems. Known methods for restriction of access to data in contemporary systems include authentication of user identities, control of access to both data files and main memory, and restriction of permitted computational actions. Such protective measures can be defeated in current environments by sufficiently skilled intruders with access to the system.

For that reason, there is a need for protection of equity in such commercial products as computer-based data. This need cannot be wholly satisfied by any technological defenses, since there is no way in a commercial environment of eliminating subversion. Recourse and remedies are needed in law, but present legislation and precedent concerning intellectual property do not properly include computer-based

information. Additionally, legislation concerning trade secrets has been under sufficient challenge to be an unreliable form of recourse in protecting such property rights.

The technological solution to the untrustworthiness of host environments not controlled by the data compiler or vendor lies in increasing the restrictiveness of that machine-based system which is being provided. Rather than vending only data, it is necessary to market software processors and protection measures as well as the data. Changes to the host environment would be required, but the overhead to support such changes would be potentially low. Additionally, specific legal action is required to produce a framework for establishing the nature and extent of proprietory rights in such data. Such a framework must be distinct from, but consistent with present Constitutionally-based means for protection of intellectual property.

## I. INTRODUCTION

Traditionally, intellectual property has been protected by granting legal rights to exclude others from the benefit or profits of particular scientific or creative work. The nature of the exclusion has depended upon the classification of the work as scientific or creative. However, protection for each type of work is based upon recognition of a greater good to be obtained by persuasion of those capable of such noteworthy work to disclose their products than would be gained by refusing the limited-term monopoly in those works.

In general, it has not bee considered that the protection of such work would require further efforts. It was believed that the nature of such intellectual work would make its abuse largely a matter of human agency, and that normal precautions against improper taking would be sufficient. The fact that such work was intended for human comprehension--a literary work appeals to the reader, an invention is described in terms to permit duplication through human effort--appeared to confirm that human action would provide the means as well as the motive for any theft.

These notions have become antiquated with the development of new forms of intellectual property. We no longer restrict this term to material which is

intended for direct comprehension by persons. The development of new technologies has expanded the concept of intellectual work to include that which may be required to make machines function. No longer is "machinery" considered purely mechanical. Computing machines have been functionally considered as logical devices. Such machines enable users to perform particular tasks, resembling some within the scope of human capability, with great speed and accuracy. For example, the use of computing machines enables us to solve equations in seconds which are so complex that a human mathematician could not finish the job in a lifetime.

Since these computational activities consist of applying programs to variable information, considerable human activity is involved in preparation for the machine processing. The intellectual level required to produce the program requires an ability to deal with abstractions, which is beyond the elementary functions of logic which the machine can perform. A new type of human work has evolved. That is the preparation of computing machines for processing--the production of programs and the preparation of whatever data is to be processed. This data is referred to as <u>input</u>, and is accepted by the machine in the form of electrical signals. The data in combination with the program

produces output.

An example of this process would be in the preparation of a machine to solve mathematical equations. The machine does not "know" equations. A programmer translates the equations into a series of the fundamental operations of the machine. The numeric coefficients required to solve the equations are determined, and converted into machine-readable form in order to be put into the machine. The equation may be so complex that the mathematician could not or would not have solved it by hand. However, in making it possible for the machine to solve his equations, the human being has performed the work which is uniquely his, and has relegated the automatic, repetitive work to the machine.

Previously, such intellectual work would have resulted in a product designed to be comprehended by other persons. Now, even though the work itself involves much human cognition, the purpose is to produce material for use in a machine. The machine itself may produce information for the use of human beings. It may also produce material for further processing by itself or another machine. The distinction between the human use and the machine use of information produced by human intellectual effort is not always clear.

Contemporary computing machines are capable of storing large quantities of machine-readable data. A single disc storage unit can hold fifteen millions of characters of alphanumeric data. A number of such devices can be attached to a computing system simultaneously. Additionally, such data can also be stored on removable devices such as tape or special disc packs which need to be attached to the machine only when a program calls for the data.

While we generally consider data to be the information used by a program, sometimes programes are data themselves. A program is a series of instructions which will cause the machine to perform a given task. However, programs are composed of the same elementary signals as data. Both are represented by binary elements. Both are stored on the same types of devices. Sometimes programes are acted upon by other programs, as, for example, when a program is being edited or changed using a program which edits text. In referring to data, then, we will also be including the subset of programs.

Data can be produced by human effort either directly encoded into machine-readable form, or by the intermediate operations of a program. The distinction between data and a random occurrence of binary signals

is that data was planned in order to enable a program to achieve a definite result.

The machine-readable nature of this product has changed the nature of misuse of information. Misuse and improper access are no longer accomplished by purely human agency. Misuse often involves access to the information in its machine-readable form. Therein lie both a problem and a solution. Because the data are associated with a computing machine an intruder can turn the capabilities of the machine to his use and obtain improper access to the information. The machine, however, can be programmed to protect itself. As we will see, neither the problem nor the solution are in reality quite so straightforward. However, unlike other types of intellectual work, the preparation of material for input to a computing machine involves the exposure of the product to a partially unknown and potentially dangerous audience.

There are some legal rights to conventional intellectual property. We will see that these rights do not automatically transfer to intellectual property which is intended to be processed by machines. In recent decisions of American courts dealing with current technology, material which does not fall strictly within present definitions of the patent and copyright laws has

been excluded from protection under those systems.

Additionally, it may not be possible to rely on legislation which was intended to protect against unfair practices in commerce. The use of unfair competition laws to protect intellectual property which did not fit either the patent or copyright systems has been a matter of intense controversy in some recent Supreme Court decisions.

The legal status of intellectual products which are intended for machine processing rather than human cognition is not defined at this point. In order for this type of material to be differentiated, it will be necessary to examine the framework in which recent Court decisions have rejected it from traditionaly protection. We will have to understand the motivation behind this exclusion. Then we can define a legal structure for the protection of such material which will be consistent with the purpose and methodology of protection of intellectual property in American law.

The problem of technological protection of such data is a parallel but separate problem from the issue of legal protection. These two forms of protection must be considered as complementary. Technical methods of protection increase the difficulty of an illicit use, and effectively bar all but determined intruders.

However, they can be subverted by individuals possessing a high degree of knowledge and skill. Then legal protection is a recourse in the event of the failure of the technological barrier. Legal recourse, however, is not guaranteed redress. The issues must be resolved through litigation, and the definitive statement on the rights of the parties involved comes from the courts. The application of technical defenses is necessary because the damage done by intrusion, even if legal action is successful, can be quite destructive. Legal recourse is necessary to provide a deterrent to the undertaking of a break-in, and to provide the damaged party with the hope of restitution or damages. If legal protection were the only sort available, the defense of an intruder might be that nothing was taken that was not, in fact, made available for the taking. Technical defenses would be required in order to show that the data owner did not contribute to the misuse by neglecting to protect his property.

There are three rather specific motivations for protection of computer-based data. The first is that the information may be covered under public laws which determine its sensitivity, as with data related to national defense. This is a particularly specialized situation, and we will not attempt to deal with protective measures required for government classified

material. The second motivation would be ethical considerations related to data identifiable to persons. There exist large bodies of such computer-based data. The recent public interest in privacy which resulted in some legislation concerning the obligations of credit bureaus was somewhat based on fears of possible misuse of such personal data. We shall examine some of the issues related to privacy, but this issue has been extensively covered in a number of studies and we shall not duplicate that work. The third motivation is that the usefulness or profitability of the information may be determined in part by its uniqueness and limited availability. This is the situation with which we shall be most concerned.

The situation is analogous to that which exists with respect to information intended for reception by human beings. A book is potentially profitable because it is unique, and the publisher will obtain that profit because he is the only one--for a limited time--who can legally produce that book. Should someone else, having obtained a copy of the book, decide also to publish it while the original owner's copyright is still in effect, there will be legal remedies available should a court decide to uphold the copyright. In the case of machine-readable data, we intend to demonstrate that there is presently no such legal recourse, and that one

is in fact needed to enable a viable industry in the production of such material. However, the book publisher is restricted in defense of his product to traditional methods of protection against theft. The producer of machine-readable data has available a number of technical defenses against an improper taking of his product.

Until recently, most data in machine-readable form was compiled by its owner for his own use. Recent developments in computer technology which have resulted in large and fast data stores have made attractive the possibility of associating large amounts of information with a central processor. The need for information to be used as input to programs is increasing as the number of uses of computing machines has grown. It has become recognized that the costs in machine time and human talent of collecting data and converting it into machine-readable form can represent hundreds of thousands of dollars. Thus, the existence of a market for commercially produced information in machine-readable form has become recognized. The development of such data bases in response to specific customer needs, as well as the production of general information collections, has become an attractive enterprise. However, marketing such data requires that there exist safeguards to ensure that the contractual

basis for the use of such intangible material is not violated. The need for preserving the integrity and privacy of such a product is great.

We will examine the legal and technical problems involved in providing such safeguards. We will propose systems for providing protection, first of all in the technological area, and then in the legal area, which are consistent with the precedents and capabilities currently existing in each area.

## II. PROTECTION WITHIN THE COMPUTER SYSTEM: THE STATE OF THE ART

In order to understand the nature of potential threats to computer-based information and the defenses available, it is necessary to review the principles of operation of a computing system. The basic elements of such a system are the central processor, the memory, storage units, and control devices. The processor executes the machine instructions. Memory is accessible to the processor, and holds the instructions and the data. The storage devices hold machine-readable information which is not directly accessible to the processor, but which is available to be read into the memory. The control units manage interactions between the processor and memory, and between storage and memory.

This hardware functions under the control of a program which is known as the operating system. It controls the behavior of other programs--user programs--which perform the specific tasks which the machine was obtained to carry out. The operating system allocates machine resources to user programs, and protects itself from errors in those programs. It also prevents the user from committing errors of certain types which would affect his results. For example, user

programs are trapped by hardware--aborted abnormally or prohibited from the specific action--if they try to access memory beyond their range, use resources which have not been previously defined to the system, or exhaust their allotted time on the machine. Some traps are designed to prevent arithmetic impossibilities, such as division by zero.

The way in which user programs are entered into the machine depends upon the mode of operation of the system. The original mode was single-user batch processing. In that mode, jobs are put into the machine from a central site one at a time. Each job has access to the entire facilities of the machine. Slightly more sophisticated batch systems overlap computation with input/output so that resources would be more efficiently used. However, that is dependent upon the particular bias of the user program.

Changes in hardware design and operating system technology have made possible more efficient operation of computer systems. Now operating systems can serve multiple, simultaneous users. There are two ways in which this is done. Several processors may be combined in one system, with jobs scheduled on both processors, or a single processor may be made to execute several jobs at once. This involves a complex resource

allocation and scheduling algorithm. In such a system a program makes a number of trips between storage and memory before it finishes executing. The trips represent time slices which are made available to the program. These techniques for permitting numbers of users to execute programs at one time have resulted in very efficient use of computer systems.

This type of design also made possible time-sharing systems. Time-sharing permits individual users to interact directly with the computer on a basis that appears to give instantaneous service. Time-sharing is generally controlled by an executive which appears to the operating system like just another user program, with some advantage in competing for resources. However, to the user, the executive appears to give him control of all facilities of the system at any time he may request them. In order for use of this executive to be feasible, the way in which storage was managed had to change.

With the introduction of time-sharing, central site operators cannot depend upon being able to schedule job input. The user, through a communications line and a terminal such as a Teletype, initiates his program activities at his convenience. His activities generally require access to files which may contain data or

programs to be used. In the batch mode, operators could take advantage of the sequential nature of the job stream to obtain files on removable devices such as magnetic tape and mount them on system units. In that mode users always interacted with the machine through the operators. With time-sharing, files have to be accessible to the operating system continuously so that the system will not be unnecessarily tied up when a user requests access to them. The means for doing this is a file system which associates files with users, and converts user-specified file names into the actual hardware locations of the files. The file system also permits the user th define permissions to be attached to the file for his own or other person's use. These permissions determine the ability of users to read or write on the file.

A problem unique to multiple-user systems is allocation of memory among competing programs and enforcement of assigned memory boundaries. In batch single-user systems the memory occupied by the system is known in advance, and a user is allocated the entire remaining memory in the machine. The multiple-user systems require that the system accomodate a constantly changing ratio of programs. New programs must be allocated memory from the residue left by the most recently terminated programs, and this residue is not

likely to be contiguous. Compaction of memory is required to fit new programs, assignment of new memory bounds must accompany compaction, and enforcement of these bounds is continuously required. User errors in execution must not affect concurrent programs in any way. Abnormal terminations must not cause errors in parallel processes, nor must addresses outside of a program's range be left untrapped. There are several solutions to these problems. The general solution is to enforce program relocation--assignment of addresses in the machine--via hardware, and to permit the privileged programs such as the operating system to access addresses anywhere in the machine, while user programs are checked by the relocation hardware every time they develop an address during computation.

Time-sharing systems in particular are required to know the identity of their users. While batch systems generally obtain this information from a simple job number, the time-sharing system needs a way to identify a user and his files. The accounting system can use this identification to charge each user for his direct demands on resources. Enforcement of previously determined file use permissions also requires identification of the user. The authentication of a user identification is generally performed by comparing the information supplied by him with a list known to the

system. This facility may be extended to batch processing as well as time-sharing by the inclusion of some additional control cards in the batch milieu. However, the interesting consequences of the authentication process occur in time-sharing and we will confine our examination to that environment when we describe threats to data security.

Originally, in single-user batch systems, the capabilities of the machine were limited. Instruction execution was slow, and data storage capability limited. Magnetic tape was the principle means of obtaining bulk data storage, and was neither convenient nor efficient. These second-generation systems were not used for processing large amounts of information, and thus misuse of data was a manageable problem. The sequential nature of job input made any misuse vulnerable to detection, and the user's interaction with the machine was limited by the intervention of the batch system.

Present third-generation systems present far greater capabilities for large-scale data processing, and far more serious threats to protection of such data. The development of extensive amounts of on-line storage for use in interactive systems has widened the area in which intrusion into private data can occur. The multiple-user characteristics of these systems has

increased their vulnerability to attack during computation. The authentication process which is intended to protect files is open to impersonation.

Problems of physical security of the computer installation can be handled by conventional techniques of facilities management, and will not be discussed here [105]. There exist both hardware and software defenses to the threats listed above. However, such protection is expensive, since it adds to the overhead of all computation by increasing the demand made on operating system interaction with user programs. Generally, protective measures also add to the difficulty of using the system. Thus, such measures are often resisted by users when they are proposed. Even if they are implemented, they can be subverted by skilled, knowledgeable persons with access to the system. Thus they add to the protection of information from outsiders, but do not present an obstacle to skilled insiders. We will consider presently available protective measures which are designed to defend against deliberate misuse of data. We will not consider protective measures which are intended to guard against hardware error, such as parity check circuits which verify the success of input or output operations.

The most accessible point for intrusion is the

authentication procedure. If the information entered is acceptable to the system then the user is permitted to proceed. There is no way in the typical time-sharing system to erify that the person entering the log-on data is not in act an impersonator. The simplest way for an illicit user to obtain passwords is if the users do not protect the confidentiality of those passwords. Users who write their passwords down or who use easily-deduced phrases for them contribute to the vulnerability of the system. However, there are techniques that can be used to obtain entry into an authentication process without first knowing the passwords.

Most log-on sequences permit retries in the event an incorrect password is typed in. This is done for the convenience of the legitimate, but befuddled, user. If the entry is still wrong after a small number of retries most systems will automatically disconnect the terminal from the communications line. However, in general, the terminal can be redialed immediately. Thus, an intruder can repeatedly retry passwords until he obtains entry to the system [50]. However, he is still faced with the problem that if the files which he needs are not associated with that password, he cannot then access them. In general, such trial and error is simply a means of gaining entry to the system to perform brute-force operations.

If the intruder has the use of a mini-computer, then the construction of passwords is less tedious. This method is most effective when portions of a password are known, and there are a few unknown characters. The mini-computer can be programmed to retry combinations of characters until it succeeds.

If this method is not workable, then an intruder can use a piggyback technique. A terminal can be inserted in a communication line between the system and one of the terminals used by legal users. After a successful authentication has been completed by a legal user, this illicit terminal intercepts communications. It sends error messages to the legal user, while communicating with the system itself. A modification of this method is to permit the user to interact, intercept his sign-off message, and continue to operate on his identification [50].

Communications lines which connect remote terminals to a central site are vulnerable to eavesdropping or wire-tapping. These techniques can be used to obtain the details of a correct authentication procedure, as well as to obtain data [76]. It is also possible to eavesdrop within the circuits of the processor by intercepting transmitted signals. Threats of this nature can be forestalled by installation of shielding

or by the regular use of "bug" detectors. Hardware devices are available which can scramble transmissions. They are effective against eavesdropping, but are vulnerable to analysis of the patterns in the scrambled material. The techniques used in such devices are cyclic alterations including frequency inversion, band splitting, amplitude scrambling, and time-division scrambling.

A method of avoiding impersonation is to make the log-on sequence a series of question-answer responses where the total set of answers is evaluated in order to determine access. This is known as the "extended hand-shake." It is inconvenient for legitimate users, but can be designed to exclude intruders by extracting answers to queries that only the set of legal users could match. For example, personal data about the users might be included in the series.

Some systems only permit passwords to be used once. Users either compute their new passwords, or are informed by presumably secure means as to the new ones. This method is safe from eavesdropping, since even if a password is detected it is no longer useful. However, if the persons involved are tempted to write down the passwords because of the increased difficulty in remembering a constantly changing set of data, then the

security of the system can be compromised by conventional trespass and theft. If passwords are computed, then the algorithm and parameters used to compute the passwords must be protected [7].

The intent in protection systems is to increase the work factor of penetration of the system to the point where the value of the data obtained is not worth the effort. This is not possible without increasing the cost of normal use of the system. A log-on system which discriminates among users and identifies impersonation would be feasible but would require complex modifications to the system and the addition of specialized hardware. Such systems would include voice-recognition systems or fingerprint identification. In addition, it is possible that the system might reject legitimate users, if, say, a voice recognition systems did not allow for having a head cold.

An alternative method for dealing with misuse of log-on identification is to only permit certain pre-defined terminals to be used for particular operations. For example, only terminals physically located in the payroll department might be used to perform activities using salary files. In order to enforce such restrictions, the terminals so designated would have to be hardwired into the system. Otherwise

it would be possible for other users to simulate the identification of the restricted terminals. Only a small number of terminals can be so restricted since the available ports on the controller in the central site would be quicly used up. Additionally, the restricted terminal must be so secured that only personnel who may perform tasks of that nature have access to it.

The interconnection between the authentication process and the controls used by the file system in time-sharing systems means that once the user has completed log-on successfully, he is able to access the files associated with that identification. His access may be limited by the permissions attached to the files. However, granting permission to access a file gives access to all the contents of a file. Since input/output access is defined at the file level by associating file locations with permissions it is not possible to provide a more refined permissions list at a hierarchically lower level than the file.

Some system designers have suggested that it would be more efficient if files could be distinguished as data-dependent and data-independent in order for access restrictions to be more selectively imposed [21]. Permission to use a data-dependent file would have to be checked every time the file is referenced, as is

presently done. If the file were data-independent, then permission to use it need only be obtained the first time it is referenced.

Verification of permissions in that environment would require considerable change to the user's computing system. These changes would be costly and inconvenient. What is proposed in that system is to perform permission checking in two places instead of one as is normally done. The access-right checking for data-dependent files would be carried out as is presently done. The checking of permissions for data-independent files would become a function of the translators in the system--the assemblers and compilers. These programs traditionally check the syntax and semantics of the program and translate it into machine language, incorporating references to system routines which may be necessary to carry out tasks such as input/output. They are considered to be free of any constraints based on local characteristics of the system of hardware. Thus, a compiler supplied by a manufacturer can be used by any installation using that vendor's equipment.

Advocates of double file access checking reason that having verification of access rights to data-independent files carried out in the translation

process would reduce run-time overhead by eliminating verification at that time. The overhead introduced by this double access checking is also high since the modifications required in order to do the checking at compilation time would be difficult. Translation programs are almost always supplyed by the machine vendor and incorporation of local changes would require substantial talent. Additionally the file system would have to be modified in order to recognize the distinction between data-dependent and independent files.

Although it is suggested that the overhead will be lower in such a system since fewer checks are made, it is still necessary to check in order to see if it is necessary to check the permissions. It is difficult to see how any real gains will be made in a system such as the one proposed. The same methods of intrusion that would work in a conventional system would work in the one scribed above. Modification of the checking routines or the compiler would permit intrusion. Thus, no gains in actual data security are realized.

There are also two objections in principle to the philosophy of this proposal. The first is that translation programs suffer enough from non-standardization. The problems in communicating and

sharing programs between installations are greatly aggravated by the inability of programs compiled on one vendor's equipment to run on another. A proposal which intends to add further local modifications to translators ought to be rejected.

The second objection in principle is that this proposal ignores the distinction between logical references to files and definitions of physical addresses for those files. A considerable advance in program generality was obtained when it was realized that it was possible to make an arbitrary file reference in a program, and not bind that reference to a physical file until execution time. The proposal above goes backwards from that point, and demands identification of the physical file and its contents at translation time.

Any system which requires that data be examined in order to verify whether or not a particular user is able to access that information is vulnerable to intrusion. There must be a program which read the protected file and determines whether it is possible to honor the input/output request of the user. That program itself can be subverted. Such an intrusion is referred to as a Trojan Horse--the system program which is assumed to protect the file has been transformed into an illicit process. Knowledge of the function of that part of the

system and free access to those programs is necessary to implement a Trojan Horse. If it is assumed that certain files aren't checked, that fact can be of use to an intruder who can use his knowledge of the implementation of the checking algorithm to simulate a similar stopping order on files he wishes to access.

No matter how ingenious the protective system for a particular installation may be, it is still necessary to be able to ensure the accuracy of those elements of the operatng system which have access to the protected files. If those access modules can be modified or replaced by an intruder then the entire security system is defeated. The problem of determining that programs--system or user--actually perform the tasks that they are intended to and no others is the problem of certification [41]. It is an attempt to demonstrate by logical means that the system is correct. That is, techniques in program proving are used in order to show that the program in fact performs as stated.

Certification can also be required for hardware, although it is then accomplished more directly. The detection of security weaknesses in control logic can show what elements can be checked by software, and what elements require redundant circuitry for protection [67]. Failures in hardware can result in trapdoors

being opened onto otherwise secure systems for use by a knowledgeable intruder.

Software can be certified by inspection of code if the system is divided into modules each of manageable size. Exhaustive testing also produces good results. However, while continuous tests are possible of hardware circuits to ensure that they are not subverted, continuous testing of software is extremely impractical. Extremely careful restriction of access to system programs and the system library are necessary in order to guard against substitution for legitimate modules.

The operating system is a particularly attractive intrusion point. Since many current systems operate in dual modes where the user is under control but the system which oversees the user has unlimited access within the machine, subversion of elements of the operating system permits an intruder wide license. Hardware subversion to accomplish this end is a distinct possibility, and there should be regular software tests to ensure that the circuitry has not been altered.

In addition to the internal threats, data which is transmitted over communications channels is vulnerable to interception. The use of time-sharing has made the use of remote terminals common, and recent computer networks represent similar opportunities for

interception. If interception of transmission is considered a real threat, then implementation of cryptographic systems should be considered

Data is encrypted either by transposition or substitution of characters [53]. Transposition techniques are quite easy to decode and will not be discussed here. There are a variety of substitution techniques available [99]. Some methods are vulnerable to systematic methods of solution, such as the Vigenere cipher, which is a polyalphabetic substitution. While this offers a number of encipherments for each plaintext character, with sufficiently long text patterns will be repeated which will divulge the key and the text.

A method which cannot be broken by cryptanalysis, given a sufficiently long key, is the Vernam cipher. This requires that the data be represented in binary form. The key must be as long or longer than the plaintext. The text and key are logically combined in the operation known as "exclusive or" to produce the enciphered text. This operation consists of setting "on" all binary elements where both the key and text were "on" and setting all other elements "off". The same operation of exclusive-or is used to decode the text using the same key. This key cannot be broken by analysis because it does not produce patterns of

repeateed enciphered text which correspond to characters when the key is properly chosen [86].

Other techniques have also been proposed [14,17]. The particular operation and constraints of memory and speed would be considerations in selecting a particular encoding scheme. The combination of cryptographic techniques with other security measures is often necessary [6]. Encryption alone is secure only if it can be determined that there is a single, known, weak point in an otherwise safe system. Once such a method is chosen it is then necessary to introduce measures to protect the encryption routines and the keys [76].

Techniques which protect access to files and communication channels still leave data vulnerable while it is being processed by legitimate programs in memory. concurrent user programs in multi-program environments, or even service routines provided by a system, can threaten the integrity of information in the user's memory area. Some possibilities for such interference are listed below:

1. A program can exceed its memory bounds and gain access to the memory allocated another program, thus obtaining data.

2. A service program called by a legal process can leak data belonging to that user to some other party.

3. The operating system which controls the user program can be subverted to leak data.

We have discussed problems of type three previously. There are a number of ways in which the first threat can occur. In higher-level programming languages--compiler languages--data arrays can be referenced by subscripts. If a variable subscript assumes a value sufficiently out of range it might refer to an area in use by another program. Similarly, in assembly-level language an address modification operation may place the developed address within the range of another program. Such errors can be halted by hardware checks of all developed addresses during execution. If such checking is not performed then programs can exceed their memory ranges and encroach upon other processes. Most multi-program systems perform such hardware address checks and reject all attempts to access areas beyond memory limits.

The second situation listed is of particular interest. Legal programs may need to call service or utility programs to perform functions which are not within the power of the user program. These subprograms are unknown to the legitimate user and require specific techniques to prevent subversion of the user's program or data [57,83]. (They are unknown to the user in general because he assumes the functions they perform to exist without requiring his knowledge of the specific

mechanisms required.) Some specific actions which may be attempted by service programs are:

1. The data can be copied onto a file belonging to an intruder, or onto a temporary file for concurrent processing by the intruder.

2. If the service has memory, it can save data and pass it to its owner on request.

3. The service can use system interprocess control facilities to leak data.

4. The service can encode data in the bill which it presents for its services--a copy must go to its owner.

5. File interlocks preventing simultaneous use of a file for reading and writing can be used as a shared Boolean variable to communicate data.

6. Activities such as paging rate or ratio of input/output to computation can be used to transmit data. The only way to prevent such intrusion is to require that service programs be confined [57]. That is, utilities may not control the use of system facilities such as input or paging and they may not have memory. This confinement must be enforced by the operating system. Since an intruder with access to the library where system routines are stored can substitute a malicious program for a routine designed to provide a service it is necessary that the actions of unknown programs be restricted whenever a user is required to call on them.

The concept of restriction of the capabilities of programs shows promise as a means of increasing the

security of information. A process is assigned a segment or ring in which it may function. Associated with that ring is a set of capabilities [41,42,58,82]. Each distinct ring permits different capabilities. There is an ordering in which the power of the capabilities increases. Programs are only permitted to traverse rings in the direction of decreasing capabilities. In other words, no program may increase its power by changing its region of operation. Since restriction of a program to a region can be rigorously performed by hardware, it is possible to make access to the name of a capability equivalent to the right to execute the capability. thus, if a program resides in a ring it is permitted all the capabilities associated with that ring and no further checking of the rights of the program is necessary.

This principle is used in the Multics system, which is an experimental multiple-user computer utility designed and operated by the Massachusetts Institute of Technology and Honeywell Information Systems, Inc. It may eventually be available in systems supplied by commercial vendors. The present implementation of the ring structure is largely in software although hardware support is being developed [82]. The effectiveness of such a system lies in the division of capability levels according to reasonable estimates of functional needs.

If there were two capability levels, then the system would be an analogue of present master/slave or supervisor/problem organization of operating systems. The major disadvantage of such two-mode systems is the absolute nature of the division. The "master" mode is permitted access to all memory and use of all instructions available to the machine. The "slave" mode cannot perform operations which have been designated as "privileged." There is no way to grant partial privilege. If a program is able to obtain privilege then it may access any address within the memory of the machine. Certain master-mode operations may be made available to slave programs through vectors which permit access directly to the operations desired, but those vectors do not constitute giving the program privilege. Variation in the degree of access to privileged procedures is the distinguishing characteristic of ring structures.

Some operations which are required for effective protection require privilege. It is very risky to give even a "good" program privilege in dual-mode systems. The selectivity necessary in order to regulate access to protected data requires an ability to control the operations of other programs, which is a highly privileged function. It may not be wise or efficient to make such privileged operations available to protect

files which are defined locally. A restricted capability to perform some of the functions of an access-checking program would be of use in implementing a lower level protection system.

We have seen that there indeed exist technical defenses against intrusion into protected files, but that these defenses are vulnerable to attack by persons with specialized knowledge. Errors and hardware failures can be used to provide entry points into a system in which the software is secure. It should be emphasized that error checking hardware is as susceptible to failure as other hardware, and failures may permit intrusion until the failure is detected by some intuitous means.

The major unsolvable problem in protection of information is the behavior of personnel. Innocuous system programs can be replaced with ones that threaten dta integrity by persons with access to the system library. The technical solutions are effective against errors and intrusion by outsiders or unsophisticated users. However, the potential for subversion of skilled staff exists and can defeat any of the technical solutions.

Carelessness can be minimized through administrative procedures. Personnel associated with

sensitive and valuable data should be educated as to the value of the information. Protective systems should only be revealed to those who have a need to know the details in order to perform their jobs. The temptation to use short-cuts in operating system programs when they bypass deliberate protective impediments should be strongly discouraged. The task of management is to ensure that the opportunity for misuse of technical skill to defeat protection of assets is minimized, and the motivation for observing security measures is high.

Technical defenses in a computing environment can be compared to the locks to a house. An unskilled person could neither pick a lock nor enter a computer system illicitly. A person with reasonable skills can break a flimsy lock. A highly skilled intruder can pick any lock, just as a knowledgeable programmer can break into a system with which he is familiar. If the burglar is given the key to the lock, he is in the position of the intruder who has obtained the detailed information needed to subvert protective mechanisms embedded in the system or the hardware. Just as an unlocked house represents an unreasonable invitation to theft, exposed information of value will most likely be taken. Conversely, given the motivation and skill of burglars it is somewhat dangerous to rely solely on locks. As we will see later, legal defenses in the event of

successful intrusion should provide the owner with the ability to recover the damage to his investment.

## III. PRESENT LEGAL REMEDIES

As we have seen, present technical methods of protection for information in computer-readable form provide a valuable deterrent but not total security. The use of such safeguards should be accompanied by enforcement of legal rights of exclusion. If the technological safeguards are defeated there must be some recourse for compensation or punishment. Without the technological defenses, legal enforcement of rights could be denied on the grounds that there was nothing taken that had not been made readily available. To extend our previous analogy, failure to lock a house would be cause for some reluctance to prosecute an ensuing burglary.

It is helpful to have some way of detecting the occurrence of questionable activity. Records of usage of protected information are helpful. Such threat monitoring procedures as logging all data changes or recording all user identifications when the file is accessed provide a way in which an audit can reveal the source and nature of dubious actions. This may reveal an attempt at intrusion. Traditional clues, such as the appearance of protected information in places where it could not have been developed independently, also provide a means of detecting such intrusion.

An obvious threat is the theft of a removable storage unit, such as magnetic tape, with information of value recorded on it. The recorded signals constitute the unique, intangible component of the property, and generally exceed in value the cost of the physical edium which contains them. Such a theft can be prosecuted under a number of precedents. In two very analogous cases in California, lists of new telephone subscribers were stolen*. The defense in each case was that the paper on which the lists were written had such a low value that the minimum required loss for prosecution for theft had not been met. Both cases were decided similarly--the value of the stolen material was created by the work of the compilers of the data, and the theft could be prosecuted. In the event that such stolen material was computer-readable information it is quite likely that a similar line of reasoning would be followed.

A common threat is that the data would be copied rather than taken. Most data does not reside on easily removable devices, and copying is less likely to be detected than taking. This threat suggests that

---

People v. Dolbeer 214 Cal. App. 2d 619 29 Cal. Rptr. 573 (1 Dist. 1963).

People v. Parker 217 Cal. App. 2d 422 31 Cal. Rptr. 716 (2 Dist. 1963).

copyright protection might provide effective recourse. In fact, in 1969 the Copyright Office issued Circular 31D which describes requirements considered to be in effect for acceptance of computer programs for registration. The extension of copyright protection to other computer-readable products would seem reasonable since the use made of the copyrighted item is not an issue in determining its eligibility for copyright.

That interpretation of the Copyright Act extending its protection to computer-readable material has not been tested and affirmed through litigation. Thus it is not clear what protection would actually be afforded by registration of such material for copyright. The fact that copyright protection does not extend to cover use of the material is a disadvantage. This is particularly true in the case of computer programs, which are vulnerable to both copying and use. It cannot be predicted presently whether a copyrighted program which is executed in a computer system by an intruder is being used, or whether it would be held that the memory configuration holding the program constituted an illegal copy of the program. Until such issues are resolved through litigation, the nature of infringements and remedies in this area are largely undefined.

The situation of computer-readable data is

analogous to that of programs. Such data may eventually result in human-readable printed text after processing. However, it has a separate form of representation before processing, and is susceptible to illicit use by programs during computations as well as to copying. If such use by a program resulted in considerable alteration of the data before the results were produced, it is possible that the process would be considered use of the material rather than copying of it. In such a case, recourse under copyright would be lost. It might be argued that moving data from storage into memory, which is necessary for any computation to take place, itself constituted an act of copying. That argument would be balanced, quite correctly, by the view that this data transfer was a necessary intermediate step in the computational process, and was in fact a part of the use made of the information. At present, it is not possible to predict the outcome of those opposing views in a particular case.

In practice the issue of copying as opposed to use has been the source of considerable litigation in the copyright area, and has encompassed a wide range of subject matter. Copying is specifically prohibited in the Copyright Act for registered material.

Use is quite acceptable*.

In order to clarify the distinction between use and copying, it has been suggested that an item may have two aspects: explicative and functional [24]. The explicative aspect is that which is protected under any existing federal system, then it is protected through the patent process. Let us investigate this method of stating the problem, and apply it to the special case of computer data.

The explicative representation of data could be said to be the human-readable, or human-communicable, version of that data. Such a version can always be obtained by passing other forms of the material through special programs designed to put out the information onto such devices as an alphabetic printer. A representation so obtained might encompass visual auditory, or tactile perception. Computer-generated speech and Braille would be considered as analogous to printed text. The functional version of data would be the machine-readable, magnetic-coded representation of the material in computer storage. Those binary signals which compose the machine-readable form can only be made use of by a machine of the nature of a computer.

---

*Baker v. Selden 101 US 99 (1879).

The explicative form would be comparable to other entities which are protected by copyright. This is a form which human beings can perceive through unaided senses. The functional form underlies the explicative version, and is not intelligible to persons without the intervention of a machine process. This version exists for the purpose of being processed by programs on a computer system. Appropriate protection for the functional version of data would lie in a system specifically designed for processes.

It may be suggested that the machine-readable, binary representation of data is in fact only a translation from one language--human readable information--to another. This view requires that we accept the characterization of the machine-readable form as a "language." A language, according to Webster, is "the body of words and method of combining words used and understood by a considerable community." The set of words make up the vocabulary. The method of combining words comprises the rules of syntax. If the machine-readable vocabulary and syntax can be distinguished from those underlying constructions which were encoded into binary signals then this representation is a language. However, such a distinction cannot be made. There are no nontrivial words and rules of syntax which are themselves

intrinsically characteristic of machine-readable information. A binary string is always a representation of something else--a string of text, a number, or a machine instruction. Any binary string can in principle serve as a representation for any such item. The conversion into machine-readable form is accomplished mechanically by the use of arbitrary correspondences between the original symbols and binary patterns.

It is not possible to draw a convincing analogy between machine encoding and translation. The conversion of, say, an English novel into the French language is translation. Each is a language. Unique, meaningful statements can be made and communicated in each language. Art is required to make statements in one language linguistically pleasing in the other. If the process of encoding into machine-readable form is not a form of translation, then the rights specified in the Copyright Act to sole translation are not violated by machine representation. In fact such encoding is more comparable to conversion of handwritten material into typewritten form than it is to bona fide translation.

The functional nature of machine-readable data can be made more clear by examining the behavior of a computing machine which is processing data. In memory,

the data is represented by magnetic cores (or other devices) which are in either of two states: "on" or "off." The configuration assumed by those magnetic devices is determined by the signals transmitted when data is read from the storage devices, or when program instructions cause changes. The signals which are transmitted to the memory unit determine the state of that memory unit.

In addition to causing changes in the memory, the processor can also examine the state of memory, and take subsequent actions based upon the results of its examination. Thus, the state assumed by memory can affect the subsequent actions taken in execution of a program. To give a very simple example, the following set of operations would cause such a situation.

1. Read a number into memory from storage.
2. Examine the arithmetic sign of the number.
3. If it is zero, execute instruction Z1.
4. If it is negative, execute instruction N1.
5. If it is positive (and greater than zero). execute instruction P1.

We can give a more complex example showing how the setting of a memory segment results in varied processing of data.

When a program is reading data from storage, it wishes to know when to stop. In sequential processing, the customary stopping point is at the end of the file. This end of file condition is represented by a special data word written on the storage unit. The nature of this word varies from device to device, but it essentially is unique and cannot be mistaken for user-supplied data. Recognition of such a condition as the presence of an end-of-file requires several processing actions. First of all, the reserved binary pattern must be recognized by the input routines which then mark the fact that the end-of-file has been reached. The occurrence of the end-of-file is then communicated to the user program which requested service by the input routine. If the user program ignores the fact that the end-of-file has been signalled, it will be abnormally terminated when it requests further input services. Thus, the binary pattern used to represent or signal a condition actually causes a set of processing functions to be carried out. Although such a signal is not a machine instruction but rather is a data word, it is responsible for subsequent special behavior on the part of the instruction-processing units.

Instructions which give rise to such program control by data are of the following types:

Data movement
Arithmetic
Boolean operations
Comparison
Transfer of control.

The first four instructions cause some operation to be performed on data. The last results from a decision made as a result of such a change operation. The first three instructions directly change the content of data cells or memory segments. The current state of a memory cell is transformed. This in turn results in a change in the behavior of the processor, since the transfer of control and comparison instructions are based on the results of previous data manipulations. The program and data, then, are co-determinants in the computational process. New states are generated in the machine memory as a result of the program execution. These states in turn control further program behavior.

The behavior of the program and the data in jointly determining the state of the machine during computational removes this process from the intellectual framework which as traditionally been established for human-readable material. The use of machine-readable data in computation is in part to control the process of computing. While the eventual result of this process may be the production of material in a human-readable form, specific control by specialized programs is required to obtain any human-readable product.

Human-readable information falls more readily into the conceptual framework intended by copyright. It is intended to communicate ideas. The distinction in such material between the expression and the ideas therein is realistic. Unlike machine-readable information, human-directed information requires not only vocabulary and syntax but also the ability to call upon experience and cognition to understand the abstractions which are expressed by means of language structures. Therefore, it is possible to protect only the expression without this restricting the free use of the ideas communicated. Such a transmission of abstractions is unique to persons, and cannot be duplicated in the computational process. Certain research which appears to simulate cognition in machines in fact merely extends the ability of such machines to recognize forms and to modify computational behavior as a result of past events.

The traditional framework of copyright is designed to protect legal rights to intellectual work in such an environment where the protected material is an embodiment of a communication of abstractions. This material is intended to be perceived by human senses. The form of expression of such human-directed material is of value, and sole right to such expression is a precious commodity. In general, the means of expression of such material is considered to have artistic or

commercial value in itself, as a particularly skillful or well-wrought work.

This explicative, human-directed material differs substantially from the functional, machine-readable form of information. As we have seen above, functional representations of data in machine-readable form are not distinguishable from their content. Such data represents process control information which is part of the computation performed by the machine, even though it may also be altered in the course of such computation. The fact that there is no distinction between the content and the form of such data in terms of the computational process--i.e., computation is based solely on form, and not on any perceived recognition of meaning--removes such machine-readable material from the conceptual framework of the copyright process.

The legal status of such computational data has not yet been at issue in copyright litigation. However, the reasoning we have expressed above has in some respects been anticipated by courts confronted by related technological issues. The earliest notable case in which a distinction was made between machine and human processing was Apollo*, which concerned player piano rolls which were made from songs for which the plaintiff held copyright in the sheet music. The court held that

the piano rolls were not a copy of the sheet music, but rather a use of it, and therefore did not constitute an infringement of copyright. This decision has been much criticized in the literature, but it has not been overturned. The obsolete nature of the technology at issue has contributed in some way to general misunderstanding of the significance of the decision. The Court seems to make a distinction which is similar to our reasoning. They refuse to treat the functional aspect of an entity in the same manner as its explicative aspect. The analogy between Apollo and some hypothetical case involving computer-readable material could be made quite strongly.

A more recent case which deals with the implications of a new technology and copyright infringement is Fortnightly**. In this case a copyrighted dramatic work was transmitted through a cable television network (CATV). The original decision found that the CATV presentation had infringed on the right of the copyright holder to exclusive performance of his work. The Supreme Court reversed that finding, saying that the use of televised signals in a CATV

---

*White-Smith Music Publishing Co. v. Apollo Co. 209 US 1 (1908).
*United Artists Television Inc. v. Fortnightly Corp. 255 F. 177 (1966) reversed 392 US 290 (1968).

network was a use not enumerated in the Copyright Act of 1909 and therefore such an act was not an infringement. This decision considered the CATV apparatus a viewer rather than a broadcaster of the performance. The decision refused to extend the Copyright Act to include material that clearly was not written into the act. The Court intended that the extension of old legislation of new technology be left for the legislatures.

A subsequent case has strengthened this reasoning. In the case of Teleprompter v. CBS* the issues were similar to those in Fortnightly, but the audience for the CATV network in the former case was hundreds of miles from the original broadcast. The Court held that the distinct involved in this case did not sufficiently distinguish it from Fortnightly, and that the precedent held. That Court reaffirmed the principle that, in the case of television, "the privilege of receiving the broadcast electronic signals and converting them into the sights and sounds of the program inheres in all members of the public who have the means of doing so." Once the signal is broadcast, the mechanism which is

---

*Teleprompter Corp. v. Columbia Broadcasting System 181 USPQ 65 (1975) US (1974).

used to convert it back to a picture and sound is not relevant. It may be converted by a television set in a home or by a CATV apparatus. The signal itself is a machine-readable datum, and any use made of it is legitimate.

The reluctance of the Supreme Court to modify intellectual property laws in the light of modern technology is also reflected in the Benson* case involving patent protection for computer software. The Court stated that it was the technological issues raised by the attempt to patent computer programs as requiring action by Congress to satisfactorily resolve them. This reluctance confirms the conservative posture of Fortnightly, and represents a position similar to that expressed in Teleprompter v. CBS. The area to be subsimed under a piece of legislation cannot be arbitrarily redefined when the environment in which the stated laws exist changes through technological advance.

The dissent by Justice Fortas in the Fortnightly case contradicts that recognition of the need for conservatism on this issue. Fortas suggests that the case ought to have been resolved solely on analogical precedent. The two cases which he cited as precedents

---

*Gottschalk v. Benson 409 US 63 (1972).

were similar in circumstance. Both involved hotels which had provided radios for the entertainment of their guests.* The courts had held in both cases that the hotels had infringed on the rights of the copyright owners to exclusive performance of their works.

The analogy between these two cases and Fortnightly is not questioned. What is at issue is how far the analogy ought to be carried. (This may be the reason that Fortas' views did not prevail.) The accomodation of new technology in a legal framework which stops short of the conditions created by that technology requires a restatement of the intent of that legislation. Such a ircumstance must at times supersede even the most elegantly constructed argument based on precedent.

These recent cases directly affect the expectation of protection for computer-based data through copyright. The use of machine technology for processing this data is similar to the use of machine technology for "viewing" television signals. This form of information may also be a technological innovation which does not parallel the forms which the Copyright Act explicitly

---

*Buck v. Jewell-LaSalle Realty Co. 283 US 191 (1931). Society of European STage Authors and Composers Inc. vs. N.Y. Hotel Statler Co., 19 F. Supp. 1. (1931).

protects. Infringement and recourse are not defined in the case of information which is processed by machine.

Some counsel may feel that the expense of obtaining copyright registration is so small that it ought to be gotten as a matter of course, even though the outcome of litigation in the event of infringement is uncertain. In such a situation, statutory requirements as to deposit, marking, and publication should be paid special attention. Publication should be interpreted as meaning general availability and at least one transfer of the material. Labels should be affixed to the tapes or storage devices which contain copyrighted information indicating that the material is in fact copyrighted [34].

Since copyright protection is uncertain in the case of computer-readable materials, many data base owners rely on state unfair competition laws which protect against misuse of trade secrets. The definition of a trade secret generally accepted is:

> which is used in one's business and which gives him an opportunity to obtain an advantage over competitors who do not know or use it*

A trade secret does not represent any certification of a

---

*ALI Restatement of Torts 757 (b) (1939).

level of technological innovation. It must represent information which is not publicly known. If a trade secret is directly disclosed in a marketed product, then it is not a secret. If "reverse engineering" or breakdown of a product reveals the secret, it is similarly not a secret.

A competitor may not obtain a trade secret through the use of immoral means. If it is divulged under circumstances which commit the recipient to protect its confidentiality, then he is obligated to do so. However, a person may, without liability, discover the secret independently and then use it. The subject matter itself is not protected. The intent of trade secret laws is to protect against corporate immorality. The monopoly which is obtained on a trade secret is by virtue of its secrecy, and lasts as long as the information remains secret.

In the case of computer data bases, the proprietor is protected by such laws against piracy, trespass, or disclosure by those bound by a fiduciary duty. However, should another business construct a similar or even identical data base, whether for internal use or marketing, there would be no liability as long as the second data base was not gotten from the first by unfair practices.

This concept of unfair competition is frequency found in state law to define the reverse side of the coin which may be categorized as trade secret legislation. Trade secrets are considered to be the subjects which meet the customary definition in the Restatement of Torts. Unfair competition is the activity which is undertaken in order to obtain or actively gain access to material which may or may not be a trade secret. While trade secret laws define the nature of such secrets and the responsibilities which inhere in them, unfair competition laws attempt to control the actual use of unethical or immoral practices in pursuit of information.

In order for unfair competition laws to apply, there must be competition between the parties*. This need not be competition as understood in the conventional sense. In the case of computer-readable material, illicit use of the information could occur in two ways. First, it might be marketed in competition with its owner. Secondly, it could be used. The first case represents overt competition. The second case could be argued as restricting competition which would normally have occurred in the sense that the data owner previously had the prospect of selling his product to

---

*Borden Ice Cream Co. v. Borden Condensed Milk. 201 F 2d 510 (1912).

the person who unfairly took it [30].

The desire to regulate morality in business affairs led to the creation of another type of legislation at the state level. This was the doctrine of misappropriation. This doctrine was applied when the criteria for unfair competition litigation could not be met. In particular, it was applied in cases where the material at issue was not protectable under any other statute. It concerned the behavior of the parties exclusively. The source of this doctrine was the International News Service (INS) case, in which news gathered by INS was later republished by the Associated Press (AP)* Since the AP had obtained the news from the INS publication and had merely disseminated it later, there was no statutory recourse based on unfair competition laws. The material, having been published, was not a trade secret. Nor did copyright apply, since the news releases were not originally copyrighted. Thus, there was no justification for a claim of improper taking.

However, the court found that the AP had in fact acted immoraly. It based its decision solely on moral precepts, citing among others the precept that one shall

---

*International News Service v. Associated Press 248 US 215 (1918).

not reap where one has not sown. In other words, the decision was based solely on moral judgement. An interesting dissent by Justice Brandeis recognizes the dangers in such a decision which establishes property in intangibles which are not covered by Federal policy as implemented through patent, copyright, or other such laws. The cogency of that dissent has to some extent limited the application of this doctrine. Some in fact call the doctrine of misappropriation a "tort of last resort" [71].

That conflict between the desire to regulate the moral aspects of business and the need to be consistent with Federal policies regarding protection of intellectual property has recurred in several recent cases. The issue has become one of whether the states may protect material of that nature, or whether Federal jurisdiction preempts state laws in matters where protection of intellectual property is concerned.

This controversy was begun by two interesting cases, known as Sears and Compco*. Both defendants had constructed lamps based on the novel designs of the plaintiffs' models. The plaintiffs had not been able to

---

*Sears Roebuck and Co. v. Stiffel Co. 376 US 225 (1964).
Compco Corp. v. Day-Brite Lighting, Inc. 376 US 234 (1964).

obtain valid patents on the lamp designs, and the products were sold in the open market. However, when the lamps were copied, the originators sued the copiers under the state unfair competition laws, having no other basis for a suit.

In both cases, the Supreme Court held that when intellectual property does not qualify for Federal protection under patent or copyright statutes then it is in the public domain and may be copied at will. Since the copied lamps were clearly marked as to their source, there was no basis for a verdict that the lamp copies had been "palmed off" as the work of the originators. These decisions affirmed the principle that it is in the interest of society to foster disclosure of material which does not meet the Federal standards for protection under a limited-term monopoly. Such a monopoly would be granted when the material is of such a quality that, in order to encourage continuing production of work of that quality, the originator is given exclusive rights to use his discovery in return for disclosure of the details of the work. If this standard of quality is not met, then it is against the interest of the common good for the state to give the discoverer any means of holding a monopoly of the work and avoiding disclosure of the principles.

Since the material used in Sears and Compco had been obtained on the open market, these cases did not require a distinction between protection of intellectual property and the necessity to restrain immoral conduct in business. That situation was particularly noted by the Second Circuit in Painton*. In that case, a trade secret licensee who had been paying royalties under a licensing agreement asked the court to release him from the contract since the model he was licensing was not protected under any Federal statutes. The original, highly criticized, decision affirmed his position, extending the reasoning of Sears and Compco to deny the state jurisdiction in matters of intellectual property. The appeals court reversed that finding. That course of reasoning, upheld on an appeal, would have negated state law regarding trade secrets. The appeals court found no basis for Federal intervention in the contract, especially since no patent application had been filed. Since the individuals involved certainly had the right to contract, there was no question concerning the validity of the covenant, and no consideration of public policy or Federal patent law justified any refusal to uphold the contract. It was as though the trade secret

---

*Painton and Co. v. Bourns Inc., 309 F. Supp. 271 (1970) reversed 442 F. 2d 216 (1971).

licensee had hoped to find immoral gain in invoking the doctrine of Sears and Compco. The Second Circuit, on appeal, noted this attempt and rejected it as unethical and not justified in law. In this case, the fact that intellectual property was at stake did not determine the decision of the appeals court, which concentrated on the need to protect the rights of the contracting party against the predatory intent of the licensee. Most commentators on Painton consider the original decision, which invoked Sears and Compco to uphold the position of the licensee, as quite incorrect in law as well as in fact.

Painton balanced the need to regulate commercial conduct fairly against the possibility of Federal preemption of protection of intellectual property. Total preemption by Federal jurisdictions would require that such issues be determined solely on the merits of the eligibility of the material at stake for existing forms of Federal protection. The questions as to the equities of parties at litigation, which are now decided at the State level under the fair competition laws, would tend to be ignored in favor of Federal patent policy issues.

Several subsequent cases involving unethical behavior in obtaining trade secrets have confirmed the

impression that such Federal preemption will be limited in cases where unfair competition is clearly the principle at litigation. In one case, a plaintiff installed a device for testing on the premises of a third party. Although that party knew that it was bound to confidentiality, it permitted the defendant to examine and photograph the device*. It was found that the defendant had been unjustly enriched by betrayal of the plaintiff's trade secret. There was no basis for, and no affirmation of, any Federal preemption in that case.

In a similar case, employees of a company used skills learned while employed to produce a competing product after they left to form their own company. The employees of the Minnesota Mining and Mfg.. Co. learned to manufacture a precision tape recorder, and after leaving, hired other employees with knowledge of this new process. Soon, they were producing a tape recorder similar to the original one*. The court found

---

*Servo Corp. of America v. General Electric Co., 337 F 3d 716 (1964). Cert. den. 383 US 934 (1966).

---

*Winston Research Corp. v. Minnesota Mining and Mfg. Co. 350 F.2d 134 (1965).

in this case that the relationship of confidentiality between an employer and the employees had been violated by the actions of the employees. This case, as the one described above, was decided on the basis of the conduct of the parties rather than any determination of the protection system available for the material taken.

However, in a third case involving Kewanee Oil Company, it was held that state trade secret law is preempted by Federal patent policy where the information at issue would have been patentable**. The plaintiff had not filed for a patent within one year of the invention, and therefore had not obtained a patent [112]. The defendants had previously been employed by the plaintiff, and had learned confidential manufacturing methods which they proceeded to imitate after forming their own company.

An injunction had originally been issued against their use of that process. However, an appeals court refused to affirm that injunction, since it held that Kewanee had forfeited its rights to protection of its secret manufacturing process by failing to meet the statutory requirements for filing an application for a

**Kewanee Oil Co. v. Bicron Corp. 478 F.2d 1074 (1973).

patent. Since the subject matter was held distinctly patentable, and therefore under Federal jurisdiction, it was held that the issue of conduct of the parties was not pertinent. The principle of Federal preemption was upheld in Kewanee, and the state was not permitted to protect any monopoly in intellectual property which should have been granted under Federal jurisdiction.

Kewanee was distinguished from Sears and Compco by the fact that unethical conduct had occurred. In Sears and Compco the sole issue had been the ability of unpatentable material to be protected by state unfair competition law. Even though that was an issue in Kewanee, there was the further complication that the parties had violated a responsibility for confidentiality. In Kewanee, it was further necessary to take into account the fact that, even though the material was not patented, it was in fact patentable, and therefore would have been unambiguously protected had the statutory requirements for such protection been met. The decision acknowledged that unfair actions had taken place in the violation of the confidentiality of the employer. However, since the company had deliberately failed to see Federal protection, it was held that there was no fundamental right in the confidential process, and that no justification existed for avoiding a verdict that Federal preemption in this

case was justified.

Essentially, Kewanee sharpens the distinction between preemptable and non-preemptable material. If a valid issue of conduct exists, that must not be complicated by any reasonable showing that Federal jurisdiction exists in order to be a determining factor. If there is reason to believe that there could have been Federal jurisdiction, or if there is no issue of immoral or unethical conduct, then Federal preemption will be upheld.

If the subject of the litigation is not a proper candidate for patent protection or copyright, Federal preemption is not an assured principle. Goldstein resulted in a decision that states are free to regulate matters of intellectual property which do not fall under Federal regulations for patent or copyright.

Goldstein involved piracy of sound recordings.* California had a statute which prohibited copying and resale of sound recordings fixed before February 15, 1972--the data the revised Copyright Act protected such recordings. The court was asked In this case to set aside a conviction penalizing persons sentenced under the California statute on the grounds that Federal

---

*Goldstein v. California 412 US 546 (1973).

preemption prohibited states from protecting material which Federal policy placed in the public domain. In a 5-to-4 decision the Supreme Court refused to set aside the conviction. The Court held that the fact that the material was not eligible for Federal protection did not disqualify local jurisdictions from enacting statutes to protect such property. In other words, it held that the Constitutional mandate* to provide patent and copyright protection under Federal jurisdiction did not prevent states from enacting legislation for protection of intellectual property which did not fall under the Federal mandate.

The dissent in Goldstein held that Federal preemption represents the only way to obtain national uniformity under the patent and copyright laws. That was in fact the justification used in Sears and Compco for denying jurisdiction to the state. Additionally, it was stated in the dissent that the failure of Congress to enumerate a form of particular intellectual property in the statutes indicated that it felt that free competition should prevail, rather than that the states should device their own protective legislation.

*Constitution of the United States, Art. I. Sec. 8 c. 8.

The majority held that the restrictions in the patent clause in the Constitution applied only to Congress. The states, therefore, are free to devise whatever criteria for protection they feel proper. A state legislature can, then, enact any form of protective laws--civil or penal--which it deems appropriate.

Goldstein may give rise to several categories of candidate material for such special legislation, including computer programs and other computer products [56]. The nature of the commerce within a particular state might greatly influence what such property it would protect. Such a legislative tool could be used to attract industries that were deemed desirable.

Presently, the situation as regards protection for intellectual property in the form of computer-readable data is not defined. Trade secret protection is viable under circumstances in which there is no Federal interest and the behavior of the parties is at issue. In the face of recent controversial decisions on such matters, it is difficult to predict the outcome of trade secret litigation. The licensing of trade secrets is still an attractive means of obtaining the benefits of disclosure without losing the advantage of trade secret status [64]. However, a freely marketed product cannot

be a trade secret. If material is not a trade secret, then protection from misuse must be obtained through unfair competition or misappropriation laws. The issue of Federal preemption raises the prospect that such issues would not be considered as weighty if there were a clear case for a Federal interest in the matter.

There is a possibility of individual states legislating their own protective systems for selected forms of intellectual property. However, since most computer commerce is not restricted by geographic bounds, it is difficult to predict what the consequences of such legislation on trade in computer services would be. Until this option is actually exercised and tested through litigation it remains only speculation.

Copyright registration remains a possibility, but it is not clear what the outcome of litigation in the event of infringement of machine-readable data would be. While it appears that precedents exist which indicate that machine-processable data is not copied if it is processed by machines not authorized by the copyright holder, this conclusion has yet to be specifically upheld in litigation concerning machine-readable data. However, reasoning points so strongly in that direction that one would hesitate to protect a substantial investment by copyright alone.

A legal structure is needed which specifically addresses itself to the problems posed by machine-readable data. As long as technological defenses can be overcome, and persons subverted, the need for legal recourse is strong. If valuable data is to be created and marketed at great cost, the vendor must have assurance that his equity is not to be taken lightly. A product which is vulnerable to misuse and improper taking requires adequate protection to make the risk of loss no greater than that in conventional business enterprises.

The data base producer who does not market his information is not in a markedly stronger position. He may claim trade secret protection for his information--unless a strong Federal interest is shown in that type of material. He may control more accurately the risks to which his product is exposed. However, he is also vulnerable to intrusion and subversion within his organization, and must also have recourse in the event that his data are misused.

## IV. THE INTEREST AT STAKE

The term "information" as we have been using it encompasses a wide variety of subject matter, formats and usages. In discussing protection of computer-based information, we are concerned with providing protection for the integrity and privacy of such data, regardless of the specific content of the protected file. We use integrity to mean the maintenance of the data without unauthorized alteration, and privacy to mean restriction of access to the data. In some cases, an intruder may wish to copy or process information which he is not entitled to have access to. In other cases, it may be useful to him to change information on the file which he illicitly accesses. In general, the problem of protecting privacy is the general problem, and integrity of data is a special case of violation of privacy. It is not possible to change information without obtaining access to it, and if the integrity of data is destroyed, its privacy has been violated.

There may be a variety of interests vested in that information and the interests desiring privacy may be in conflict with interests which require disclosure. The nature of the information which is protected determines to some extent the interests which vest in it. There are three general categories of information which may be

in machine-readable files. They are: personal, technical, and commercial. Personal information is data either specific to persons or derived from information specific to persons. Such data can be similar to that in credit bureaus or results from the U.S. Census. Technical information is related to research and development. It may consist of data about nature, descriptions of investigations or reports summarizing scientific literature, results of experiments or numeric data about particular events. Commercial information is related to the conduct of business. It includes financial data, customer lists, parts lists and other information specific to a particular business or industry.

All types of data are of particular value to their originator or owner. The owner's interests are the traditional ones of the entrepreneur. He may market the information or use it privately. He has no direct measure of its value, but the uniqueness and effort in compilation of the data are important elements in establishing a value. The difficulty which the owner would experience if he were deprived of that information, or the damage to his business if the information were publicly available are also criteria useful in measuring information worth.

If the data are compiled for the owner's use and are not intended to be publicly available, then the need for protection of privacy and legal recourse in the event of intrusion are clear. Data which is intended to be marketed is also vulnerable to misuse. The possibility of interception by third parties while the information is in the possession of a legitimate second party is a threat. Additionally, the ability of a legitimate user to contract for certain applications and to then use the information in ways which were not specified in the usage agreement is potentially damaging. It is still necessary to protect public information as well as private data.

Competitors and potential customers have an interest in obtaining the information which is shown to be of value. The customer is willing to obtain it throughugh normal channels. The competitor wishes to develop such material independently in order to improve his own competitive position and to compete equally. Failing the ability to develop the information, it is possible that he may resort to unethical means to obtain it. A customer may also wish to obtain the product at low cost, and may encourage the use of such means. Additionally, if the information is not made available on the market, then potential users may have a strong self-interest in penetrating the protective systems

surrounding it.

If information is of the personal category, subjects of the data collection have an interest in restricting the data about themselves which is collected, and the use which is made of it. A similar interest may be vested in corporate entities which must report data concerning their activities to regulatory agencies or other bodies of government. The interest of the individual in protecting his privacy there is in conflict with the interest of an entrepreneur in developing a viable business enterprise based on such data.

Technical information may be subject to a Federal interest which stems from the patent clause of the Constitution. As we saw in Chapter III, the mandate for disclosure of valuable discoveries permits the granting of limited-term monopolies for work of a pre-determined character. However, it has been interpreted as also meaning that work which does not meet criteria for such Federal protection is in the public domain and cannot be protected by other means once it has been publicly disclosed. Thus, the government interest in promoting disclosure of inventions can override other legal steps which a data base owner might take to restrict access to the data.

The selection of the correct legal framework for protection of such material, and the investment in technological safeguards varies according to the owner's determination of the threat to the privacy of his material, the value of his product, and the usefulness of alternative protective measures. In order to obtain Federal protection, the work must be disclosed. This requirement must be balanced against the possibility that disclosure may be made, and then Federal protection may be deemed not appropriate for that material. Also, the proprietory interest in protection for the information might in some cases exceed the period of the limited-term monopoly granted by the government.

In the case of personal or commercial data, the failure of a data base owner to secure his information suitably may cause liabilities to others in the event of intrusion or misuse. Personal data in particular may require that the data collector take particular precautions to prevent violation of the civil rights of the data subjects. This problem is generally subsumed under the heading of "the right to privacy." This right has been defined as:

> much he will share with others his thoughts, his feelings, and the facts of his personal life [69].

This right is not specifically mentioned among

Constitutionally granted civil rights. However, the Constitution states that the enumeration of certain rights therein does not deny or lessen others retained by the people.* It is generally accepted that there is a human need for distance between oneself and others and that society recognizes this need and accords it status as a right [108]. In 1890 Louis Brandeis co-authored a classic law review paper on this right [12], and advocated creation of a tort of invasion of privacy to provide recourse. The right to privacy is still being defined through legislation. The present state of the art in automatic data processing has permitted the establishment of large files concerning persons, and this right to privacy is becoming increasingly a matter of public concern in the face of that processing capability.

Two well-known cases which appeared to deal with the right to privacy in fact were not decided on that issue. In the case of Time, Inc. v Hill**, the substantive issue was the right of freedom of the press. The Hill family had undergone a widely-publicized ordeal at the hands of escaped criminals, and the magazine

---

*Constitution of the United States. Articles In Amendment IX.
**Time, Inc. v. Hill 385 US 374 (1967).

described a dramatization of this event. The decision upheld the right of public information.

The case of Pearson v. Dodd* was based on the actions of some employees of Pearson who entered premises belonging to Dodd and obtained documents which were relevant to the personal finances of Dodd. The case was based on the theory of intrusion, which is the right to be protected against certain methods of obtaining information, rather than the right to withhold such information [65]. Since Pearson had not himself removed the documents, he was held not to have committed intrusion and the case was decided in his favor. This case also avoided the direct issue of a right to privacy in the particular information which had been taken.

Congressional hearings on credit bureaus revealed that some contemporary assaults on privacy are based on the ability to use modern technology. Information services which determined the eligibility of individuals for personal credit did not contain adequate safeguards for personal privacy [96]. Specifically, the individuals concerned were not able to determine what was in the file about them, nor to correct erroneous statements or challenge damaging material. Such

---

*Pearson v. Dodd 410 F. 2d 701 (1969).

encroachments motivated the passage of legislation to remedy that situation. The Fair Credit Reporting Act of 1970* defines the responsibilities of proprietors of credit data bases to the subjects of their files. The act is

> to require that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance and other information in a manner which is fair and equitable to the consumer with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information in accordance with the requirements of this title.

While the individual may have willingly submitted information to a credit bureau in order to obtain some benefit, this data may still be misused. The Fair Credit Act ensures one the right to dispute information in the data bank and to ascertain what information is in fact stored about oneself. The data base owner incurs substantial obligations for the accuracy and security of his information.

Such considerations of individual privacy rights have resulted in proposed legislation extending those rights defined in the Fair Credit Act. Two such bills--not yet resolved--would create a Federal Privacy Board** to provide recourse for violations of privacy. There

---

* Pub. Law 91-508 Title VI. 1970.

** HR 9786 93rd Cong. 1st Sess.
HR 667 93rd Cong. 1st Sess.

would be regulations controlling the operation, responsiveness, and accessibility of all automatically processed files containing data about individuals.

It appears that any protective measures intended to protect personal privacy will require separation from measures intended to promote commerce. Those two interests appear to be irreconcilable. The desire to increase one's market and to lower one's operating costs does not leave room for accommodation of a desire to serve a social need and protect personal privacy. In describing the legislation undertaken and proposed for protection of personal interests in a commercial data collection situation, we intend to demonstrate that the interests have in fact been presently held to be irreconcilable. Individual rights represent a consideration which, if protected, are of sufficient value in our society to be protected at great cost when they conflict with other interests. We feel that the present trend in legislation particular to protection of personal rights will continue, and that this trend is of greater benefit to society than the possible intermingling of protective measures intended to serve both social and commercial interests. In making our recommendations for legislation to protect commercial data rights we will, then, be excluding that class of

data which concerns persons or which contains facts directly traceable to individuals. Such material will not be intended to be included in the system that will be proposed. We feel that it is more correct to require that such material be handled with regard to its special nature, and with special concern as to the civil rights of the data subjects.

Such concern extends beyond the narrow scope of credit bureau operation. However, the visibility and volume of the operations of these bureaus have caused legislators to define their concerns through privacy-protecting regulations. In such situations it was necessary for legislators to balance the commercial interests of groups such as credit bureaus against the civil rights of the persons involved. Such a restriction in the commercial use of personal data is possible in other areas also. While there are valid interests in free distribution of information--an individual who desires credit submits voluntarily to the dissemination process--the ability of the person to retain some control over that process is important.

There is some evidence that confidentiality and security are no less well managed at this time in

automatic systems than they are in predecessor manual systems. The conversion to automatic processing in 55 information systems studied by Alan Westin [110] did not degrade or eliminate the precautions which had been set up for those systems. He says:

> of personal information that civil-liberties spokesmen believed to be taking place as a direct and inexorable consequence of computerization are not happening as yet in the advanced computerizing organizations that we examined. Similarly, there has not been the ebbing away of procedural and substantive due process that civil-liberties commentators assumed to be an inevitable result of automated information handling. ...pre-existing norms and practices have been closely reproduced in the computerized systems; and where new laws or policies have been enunciated affecting civil-liberties interests, the computerized operations have embodied these just as fully as the manual ones.

Although these findings are reassuring, the potential exists for future abuse. The systems studied by Westin were large-scale enterprises in industry or government. The cost of proper security measures might prove a deterrent to their incorporation in more marginal enterprises which may find information production a profitable venture. As information handling techniques become more efficient and sophisticated the development

of data collections can be expected to grow through a broad spectrum of industry.

Maintenance of free competition requires that individuals sometimes compromise their interests. Such compromise can be expressed in contracts, regulation of actions through legislation, or by the outcome of civil action. This modification of behavior is a result of a strong interest on the part of our society in promoting free competition, and in ensuing behavior on the part of competing parties which advances competition. It has been said that, in act, a Constitutional Mandate exists for the advancement of free competition [39]. This mandate is part of the motivation for the decisions in Sears and Compco in which the need to protect the property of persons was found subordinate to the need to promote free competition. Thus the interests of proprietors in maximizing their profit and reducing competition conflicts with the interest of society in obtaining greater competition.

Society also maintains an interest in the free dissemination of information. This mandate stems from the patent clause of the Constitution, where it provides justification for the establishment of limited-term monopolies for material which meets the criteria established and which is publicly disclosed. Material

which does not meet the pre-determined criteria does not receive Federal protection. If it becomes public knowledge, then it is in the public domain. The dissemination of information through this policy of promoting disclosure in turn fosters free competition. For protected materials, disclosure of the technology aids in the development of alternative or superior works.

While it may be in the interest of the individual to enter in competition, it is also in the interest of society to encourage him to do so. Thus, there is a personal advantage to be gained by sacrificing the desire for unlimited monopoly in exchange for the support of government institutions. Similarly, the individual has a right to control the dissemination about information which is private to him, and the protection of civil liberties is in the interest of society in that it maintains a free society. While it may be in the interest of the individual to enter into competition, it is also in the interest of society to encourage him to do so. The rights of the owner of a personal data bank must be subordinated to those interest.

Any legal framework designed for protection of information must to us recognize multiple conflicting

interests. The broad structure encompassing these interests can be described as follows:

1. information owner: reasonable assurance of protection against predatory or wrongful taking of his product: participation in the market place when desired.

2. information users: ability to learn of the data; ability to compete in the market with or by means of this product.

3. information subjects: ability to control the degree or particulars of their participation; be able to challenge information about themselves.

4. society: communication of information; free competition; maintenance of civil liberties.

If legal requirements are defined to ensure that these rights are balanced and respected in information products, technological safeguards required to implement those requirements will be developed. Protection of privacy and integrity will be components of defined rights in information banks. If technological implementation of such safeguards is not forthcoming, it may be compelled as a result of legislative reaction to public concern.

Authority required to control safety has been found when the public well-being required. Industries such as food and drugs, automobile manufacturing, and general

aviation have found themselves under Federal regulation when that was found necessary to the protection of public welfare.

It is likely that the further development of information industries will similarly affect the public well-being. If the implementation and continued development of systems which are secure and protect the interests at stake in the computer-based data is not forthcoming, then it may well be required by legislation. Additionally, it is possible that, as in the area of automotive safety, the specific implementation may be dictated by the legislation. It is difficult to predict what form the airbag of the information industry would take; it is not difficulty, however, to envision requirements of that severe a nature being forced upon a reluctant industry.

## V. PROPOSED TECHNICAL SOLUTIONS

Since commercially vended machine-readable data are used in computing environments over which the vendor exercises no direct control, he is not able to ensure that hardware and support systems of each user system will enhance the security of his product. As we saw earlier, there do exist a number of highly effective protective systems. However, these require that some fundamental operations of the computer system be altered. Such basic functions include file access procedures, log-on protocols, and memory allocation. The higher the degree of protection, the higher the overhead on each user. Users who do not directly use the protective facilities of the system also pay in overhead for the modification of the basic modules. For this reason, security measures are implemented with reluctance in many environments, and their use is resisted by numbers of users.

We propose a reconsideration of priorities. We recommend that the specific system of information which is of concern be protected, and that there not be an attempt to provide generalized protection for the entire data set of the computing system. We propose that the use of a commercial data product be accompanied by contractual specification of permissible operations on

that product, and that the software to perform those operations be an integral part of the vended system. Those protective mechanisms in the data system would not extend to other activities of the host computer. The vendor would make available data plus the means of ensuring the privacy of his product.

The software included in the data system would consist of an executive which would control subprograms which directed the transaction capability which was defined as part of the usage agreement. Such transactions in general would permit:

1. Retrieval of individual items meeting user-specified criteria.
2. Production of reports in user-determined format, incorporating any or all of the contents of the data base, and providing for any computations required in achieving such reports.
3. Updating the data base with new or modified information.

These activities can be summarized as interrogation, report generation, and updating.

The provision of the executive means that the user would not be free to define his own operations on the data base after the completion of the usage agreement. Nor would he be able to implement his own software. This restriction is central to our proposal for providing security for the commercial product. While

the conventional licensing agreement may specify operations which may be performed on the product, they do not provide any meaningful way of enforcing those limitations. The provision of a total data system contains enforcing measures. In addition, the data system would include the software necessary to interact with the host computer and its operating system.

The executive would be considered by that operaaing system as another user program, but one with special privileges. This would be necessary to manage the functions which would be required in such a data system. These include management of terminal interaction, private input/output procedures, editing and formatting and of course, data protection. In order to accomplish its ends, the executive must control activity scheduling within its transaction capability, allocation of system resources, performance of physical input and output, and the transfer of parameters. Some assistance from the operating system is required for an effective data system. However, we will keep this interaction with the host environment to a minimum. The data system will be used as a distinct entity. The cost of protection of data thus becomes a direct part of the cost of its acquisition and use.

We distinguish this data system from what is

referred to as generalized data base management [19]. Data base management systems are oriented towards convenient and efficient access to data. We are oriented towards restriction of access to data in the interests of protecting the value of the information. The steps which users must take in order to conform to this protective structure involve a certain amount of inefficiency, and thus the particular use of the data system is deliberately loaded with some overhead.

We extend the definition of a data structure from the passive, appearance-defining elements such as record size and file organization to include as well the operational elements required to use the files. This expanded view fits in with the orientation of the customer, who necessarily envisions the application of the information as well as the appearance of the information when he contracts to obtain it. Thus, in defining the structure as including the software to accomplish those applications, we obtain a means of specifying precisely what the behavior of the data system will be.

The executive would perform one task which was not in the immediate service of its customer. That would be creation of its own data records. It must maintain log and audit trail records. The log generally contains the

physical image, on another storage device, of records in which a value has been changed. Often, the record is stored both before and after the change. The audit is normally a trace of transactions leading up to a change in the file [19]. These records are useful not only in detecting the particulars of improper changes, but in restoring the data system in the event of host system crashes [7,105]. The executive can provide some protection without requiring that all data be dumped periodically onto a back-up file [107]. In our case, we would have the audit record the identification of all users who access the system. Thus a history of the users would be available for tracing the source of improper activity.

In order for the executive to properly keep the audit and log, it must be able to identify all transactions which will result in changes to the data base. This is materially aided by our requirement that only system-provided software be permitted to access the data. In addition, if it is to be required that all user identifications be recorded then it is possible that even transactions which read, and do not change the data will have to be intercepted by the record-keeping routines to be embedded in the proper places in the basic input/output functions.

Additionally, the executive must restrict the programs that can access the data base. In order to do this, it must have assistance from the operating system. The basic input/output capabilities in third-generation machines are enacted by the operating system and not the user program, which merely submits a request for such service to the system. We would modify this input/output capability so that the address of the desired data on secondary storage is examined to see if it is within the protected area of the data system, and if it is, then the origin of the requesting program must be verified as a member of the data system. If the program is not within the dta system, then it must be aborted, after the nature of the intrusion is recorded on the audit trail. If the program is within the data system, it is permitted to do its input/output. Of course, if the data address had not been within the data system then no further checking would have been done.

Precautions should be taken that the physical device used to store the data is one in which such address checking is meaningful. The use of removable devices--tapes or disc units--is self-defeating. The definition of the hardware addresses to be checked can be done at the time the data system is installed, and that information should reside in protected memory where it cannot be changed except by designated staff.

Verification of the origin of programs requires a few more steps than checking the address to be read on storage units. First, there must be a code sequence which finds the return address of the calling program--which must always be provided so that it may get control back. Then that address must be checked against a pre-determined template which contains the limits of the legitimate area from which such requests can emanate. Therefore, there must have been some program which had restricted access and which set that template for use by the checking program.

There is always a protocol which is followed by programs in calling sub-programs. The protocol is defined in the language translators supplied with the system. While very basic machine-language programs may ignore the system protocol and use their own calling sequences, they do this only if they interact with no higher-level or system-provided routines. This protocol determines where the return address of the calling program can be located. The calling address can be obtained by simple arithmetic operations from the return address. That calling address is the one which must be checked to see if it is in the range permitted to request such actions.

Let us define operation LOCK as the setting of the

template which determines the starting and stopping addresses within which requests for access to the data system may be made. LOCK can be performed by the executive at the time it is installed, and a modified LOCK could be performed when program changes cause the addresses in the template to change. However, the existence of modified LOCK is dangerous, and should be avoided. We will assume that LOCK is irrevocable, and that it denotes absolute addresses rather than addresses which are modified by some base register.

Then a complementary operation UNLOCK is defined as the code which matches the calling address to the template. UNLOCK can have two possible results: pass or fail. Pass causes the requesting program to obtain the input/output service that it desired. Fail causes the log and audit records to be updated, and always aborts the requesting program.

Since the template addresses are absolute addresses, the comparison must be also done of absolute addresses. In machines with sensible relocation hardware, this can be done readily. The calling address is computed in relocatable form--that is, the form in which the program determines it--and then the base address or the hardware address is gotten by entry into the supervisor mode and added to the relocatable

address. Thus, the checking program either must be in the supervisor mode or must have access to that particular function in the supervisor mode of obtaining the base address--the actual hardware location--through a vector into the master mode. Such a vector enables a calling program to obtain a particular, predefined master mode function without itself being in the supervisor mode.

The LOCK and UNLOCK functions can be made safe from other user programs which may have access to that machine. However, they cannot be made safe from programs which have supervisor-mode privilege. As we saw in an earlier chapter, the dual-mode systems give unrestricted privilege in the supervisor mode, and even the use of memory restrictions and other protective measures can be subverted by knowledgeable staff with access to the supervisor mode of operation. Such subversion would necessarily be dealt with by legal means, if a legal framework were in fact established for protection of such an entity.

Systems which provide more than two levels of capability, such as those which are designed to use rings offer reasonable hardware restrictions against the execution of capabilities that a program is not entitled to use. Conceptually, in a capability-oriented system,

the use of the data system would be defined as a capability and the functions of checking data addresses, LOCK, and UNLOCK would be incorporated into a ring. However, in practice the number of distinct capabilities which may be defined in such a system is very small [82], and it would be extremely unlikely that such a scarce resource would be defined specifically to a commercial data system. In fact, the implementation in such a system might resemble the version which we described for a dual-mode system.

So far, we have concentrated on protection for the data in such a data system. The executive and its subprograms require protection of the same nature as the data which they are associated with. This can be accomplished by extending the area of the protected hardware storage region to include that portion which holds the programs. Then loading programs which move the executive's subprograms into memory would have to pass the LOCK/UNLOCK sequence. The basic parts of the executive which control the transaction capability and which are resident in memory all the time should ideally reside in protected memory. In any case, the region of memory dedicated to the executive must be constant in order for the template to be accurate.

The protection of programs in memory against

interference by other user programs is effectively performed in third-generation systems by the hardware memory allocation checking. These programs cannot be protected against supervisor-mode intrusion, as we saw previously. Administrative means would be required to lessen the possibility of interference by skilled systems staff in the activities of the data system.

Certification of the level of protection afforded by the data system executive would be the function of the vendor. He is concerned that the technological protection afforded by his system be of such a level that subversion would require a high degree of skill and privileged access into his product. Our concern with providing legal protection for such material has been precisely so that such intrusion into technical defenses can be prosecuted and remedies obtained. The vendor represents the primary interest in the privacy of his product, and would be the instigator of such action. It is his investment that must be protected, and by making him responsible for the software to guard the privacy of his own product we are using a principle of self-interest to stimulate development of a satisfactory system.

The interests of data users will be served by competition among vendors of data systems. There will

be increasing development of efficient and cost-effective data systems as there are users who are willing to pay for such sophistication. The profitability of such systems will determine the amount of talent dedicated to their development.

The host system should be required to provide conventional security measures to any data system. The systems which are used in an interactive mode should require user identification for each interaction. Communications channels used for transmission should be protected--encoding should be used if eavesdropping or tapping is considered to be a threat. All features available to user programs on the system, including memory protection and memory mode setting should be available to the data system programs.

A major contribution on the part of the data system user towards protection of the information product would be assignment of well-defined responsibilities and accountabilities for elements of the data system. It is in the interests of the vendor to obtain assurance that this is done. There should be one individual who knows the structure of the data and the procedures to carry out all available transactions. Other staff should only have the information needed to perform their specific jobs. The responsibilities for changes to the data,

re-start of transactions and restoration of the data in the event of host system failure should be in the hands of the data system administrator, who has total responsibility for the system. The assistance of the host computer system staff is of course necessary in event of failure on the part of the host system.

A major element in the development of these data systems will be the reduction of the unit cost by multiple sales. Towards this end, there will be considerable effort made to supply versions of systems which can be used on the most popular machine configurations. Since some of the data system is machine-dependent, changes in the executive and its sub-programs will be necessary to some extent for each new configuration of host computer. Such machine-dependent elements include those procedures which verify data addresses and check program element origins. Those require communication with the operating system and cannot be designed in a generalized way.

Other parts of the data system would be susceptible to a generalized design which might be used over a number of host systems. Such elements would be both more profitable and more reliable since they would be used and debugged by early users. The lack of true portability in the higher-level computer languages makes

such profitable concentration of effort highly difficult. Even in the same computer language there are features which are available on some, but not all, installations. If the computer system is one on which a standard version of a language is available, then programs written in a version using extra features will not be able to be run on that system.

In General, COBOL would be an attractive choice for the parts of the data system which could be designed in a generalized way. Installations which have much COBOL work often have special hardware which makes the running of programs written in this language very efficient. Therefore it would be economical in those environments, and the possibility of a reduced cost due to the number of units of the product sold might make up for some inefficiency in program running elsewhere. It would be possible to take advantage of the design of COBOL for manipulation of textual data and the flexible handling of data structures.

Modification of the operating system in order to communicate with the data system and to enable the executive to obtain the privileges which it needs is a specialized task which must be performed separately for each host environment. This requires cooperation from the vendors of the system software, and some vendors may

insist on providing those modifications themselves. Since it is important that such changes not affect any other functions of the host environment, the most responsible and knowledgeable person to perform those alterations is the operaaing system vendor. As data systems become more streamlined in their design and users have the opportunity to exploit the variety of possible implementations, particular system interfaces of choise will become known. It should then be possible for operating systems to provide a "plug-in" point to which such data systems can be attached.. Given the general trend for hardware vendors not to bundle software in their computing package it is not likely that the vendors themselves will attempt to market the data system packages until independent developers have established a market willing to pay for such a product.

## VI. LEGAL SOLUTIONS

There has been some concern in the literature about the lack of well-defined legal protection for computer programs. However, the same concern has not been advanced for protection of similar investments in data. We consider programs to be a special case of data, which is differentiated by its purpose and highly structured nature. This distinction may make unique the nature of protection appropriate to such material. However, programs are not the only computer products which require safeguarding. They are one easily identified and clearly valuable product.

A recent attempt at defining protection for computer programs was the recent proposed revision of the Copyright Act of 1909. This revision would have amended the act to include explicitly a definition of machine-readable copies as infringements [1,4,5,10,15,24,34,44]. While the revision attempt actually foundered on the problems posed by cable television rather than the complexities of computer products [37] this was not a compellingly successful attempt to solve the problem of protection for computer based information. The Committee on Scientific and Technical Information had in fact recommended extreme caution in proceeding with such a revision and

questioned the effectiveness of statutory copyright protection in such a case [93]. The revision as proposed would have eliminated the distinction between machine-readable and human-readable material which had been made since Apollo. The underlying difficulties in determining the difference between a copy and a use of material would not have been eliminated by this redefinition. These conflicts would in fact increase due to the ambiguous nature of the machine-readable material. The issues raised in Fortnightly and Teleprompter v. CBS would be especially relevant to such a situation. The potential litigation based on the definition of a machine-readable copy as an infringement could be countered by a defense based on the precedent of those cases declaring that the material was used, not copied. It is not clear what interpretation would prevail, and specific cases would have to be litigated to determine precedents for details.

However, this attempt at revision is not expected to be reconsidered before 1975. It is questionable what the value of inclusion of computer programs specifically in the Copyright Act would be. The copying of a program into memory, as we saw earlier, is not necessarily a creation of a copy of the program. It may be a necessary aspect of use of the program. Additionally, it is possible for programs already in memory to be used

by another process without the creation of a copy. Since the real threat to proprietory interest is in that use of a program, protection against copying of such material, even specifically in machine-readable form, seems too indirect and inappropriate to be of value.

The objections to protection of programs through copyright also apply to such protection for machine-readable data. As we saw earlier, data is an active component of the process which establishes the state of the computing machine at each point in its activity. Even if the intent of the computation is to produce human-readable material, the machine-readable form is distinguishable as having a function related to that process being carried out in the machine. As is the case with programs, data may be copied from storage into memory. The same defense may be made to a claim of infringement--that this step is essential to use of the material. While data may be copied in the pure sense of the word, the distinction between that act and copying for the sake of using is not easy to define in the case of a machine-readable product. Additionally, data may be used illicitly by a program which accesses it while it is in memory being used by a legitimate process. This would not cause the illicit process to generate any copy of the data. The addition of the definition of machine-readable copies as infringements of copyright

does not remove the deficiency which the traditional structure of copyright bears for protection of such machine-readable products.

For material which is not published--and publication has a very broad definition in this context--common-law copyright may be a valuable form of protection [37]. However, the interpretation of publication is generally the dissemination of any number of copies. Should copies be made publicly available then the material is held to be in the public domain and without any protection. Since the material which we are interested in is commercially marketed information, the usefulness of common-law copyright is quite limited. Certainly if material were not published, this form of copyright would protect against use since that would violate the copyright holder's right to first publication.

Detection of infringement of copyright would be difficult. The same situation applies to this material as applies to the misuse of trade secrets. The only clue would be the appearance of a product unreasonably similar to the original one or obviously dependent upon secrets obtained by misuse of a protected item. Material which is traditionally classified as copyrightable is infringed in order to be marketed in

competition. Computer-readable material may well be infringed for private use to avoid development of the same material.

A step which might be considered in the direction of obtaining copyright protection for machine-readable material was taken with passage of the Standard Reference Data Act*. This act empowers the Secretary of Commerce to compile, collect, publish, and sell reference data. The hearings which preceded passage of the act clearly indicated that the legislature intended that some of this data would exist in computer readable form: The act states:

> Notwithstanding the limitations contained in section 8 of title 17 of the United States Code, the Secretary may secure copyright and renewal thereof on behalf of the United States as author or proprietor in all or any part of any standard reference data which he prepares or makes available under this act, and may authorize the reproduction and publication thereof by others.

The copyright act originally did not permit the United States government to obtain copyright, with the exception of the Postmaster General for some material. That is amended by the above act. However, it is not

---

*Public Law 90-396 Sec. 6(a).

clear how significant this legislative specification of copyright for computer-readable material will be. The forms of protection specific to computer-based data and the nature of infringements or particular remedies are not specified.

As the investment of the business sector in computer products increased, the lack of legal protective systems for this material became a cause for concern. The Commissioner of Patents requested that industry submit suggestions for the resolution of legal problems surrounding protection of computer programs. The issue of protection for other computer material did not arise. In 1968 the International Business Machines Company submitted a proposal which described a registration system. This proposal was limited to computer programs, and offered protection for the code used in a program, but required in turn that the principles used be publicly disclosed [35]. The essential elements of this proposal are:

1. The creator submits a conceptual description of the program which is published. If this publication is used to develop a program using the same concepts, there is no liability.

2. A copy of the program is deposited with a register. This copy is kept secret for some specific period, after which it is made public.

3. Detailed descriptive documentation may be deposited along with--or after--the program

and it will also be protected.

4. No examination will be performed of deposited material other than to ensure that the format is correct. Programs will not be tested. The presence of logical or coding errors will not constitute a defense to infringement. However, if the program is written in a language which is not implementedted on any computer at the time of registration, that fact would be a defense to infringement.

5. A declaration must be filed at the time of registration identifying what parts of the program were copied from other programs, whether registered or unregistered.

6. The suggested fee for registration would be in the neighborhood of $100.

This proposal attempts to create a structure similar to that traditionally applied to copyrighted material, but designed for the particular characteristics of computer programs. Much of the methodology of the copyright structure is retained. In protecting against use of the material it makes its most significant break with the traditions of copyright.

The concepts used in the program design are specifically left in the public domain. This particular characteristic of the registration system directly derives from the copyright system, since with patent protection underlying concepts are protected. The registration system is in accord with the mandate for disclosure in the patent clause of the Constitution, since it requires that the conceptual description be

published. This registration system would have to be specifically enacted by legislation. It is not merely a revision of the Copyright Act.

Such a proposal for new legislation seems the best approach to protection of computer programs. The registration system described above provides definitions of infringements and penalties which are meaningful in terms of the material at issue. It is specifically designed for the technology which it intends to protect. The actual contribution of the implementor--the program development and testing--is protected without excluding from public use the underlying algorithm. It fits into the present structure of legal protection for intellectual property without requiring redefinition of any of the fundamental concepts which control such protection.

Presently, licensing agreements are used to control the communication of computer programs to other users. Such an arrangement holds the licensee responsible for maintaining the privacy of the product which he receives, and thus militates against disclosure of the work. In effect, licensing of such trade secrets is a means of protecting a monopoly which is obtained by virtue of the ability of the owner to keep his discovery secret. The proposed registration system offers the

ability to license programs, but requires that protection be accompanied by disclosure of the concepts.

This registration system is not appropriate for protection of computer material other than programs. It specifically addresses itself to specific elements of computer programs. Data is quite different from programs, and in fact does not stem from the implementation of an algorithm, but rather from some observation of nature or other factual material.

A weakness in the proposed program registration system becomes a fatal flaw in a data protection system. That is the failure to enumerate a method of dealing with changes in the information after it is registered. Computer programs of any complexity are rarely used over any period of time without modification. Either new efficiencies are introduced, or the computing environment changes and requires program changes, or errors are found and corrected. These changes would affect the detailed description which is deposited in the proposed registration system. However, if the changes are not basic in the program,they could be handled by submission of amended detailed descriptions. Thus the deposited material would be up to date.

In the case of information, changes would be basic to the nature of the product. If information is

altered, then it is different. Data which are collected periodically and represent new cumulations of information would pose a very particular problem. Although the generic nature of the information and the format may remain the same, the specific information would change in each period. For example, economic data provided quarterly would provide the same type of information in each period, but the numbers would change. There must be a way of distinguishing the separate versions as members of the same identity set. A descriptive method is required that will enable identification of related data in a functional manner which is not dependent upon the precise semantic content of the data base.

Finding a useful method of describing data is central to devising a means of protecting it. It is essential to know precisely what it is that is protected. Therefore, we shall first propose a way in which data can be distinguished and identified in its machine-readable form.

First, the semantic content of the data base should be described. This can be accomplished by a narrative which tells what the information is about, how often it is collected and provided, what means were used to gather it, and where it was gotten. A statement such

as: "A semi-monthly collection of citations from the technical literature in electronics obtained from the following list of English-language journals published in Japan" would meet this requirement. In some cases the method used to obtain the data would be of more interest in a narrative description. Data obtained by observation of physical processes might require a more detailed description of the technique and equipment used for its collection.

The physical arrangement of the data must be precisely described. This physical structure defines the machine-readable component of the data base. The principle distinction between human-readable and machine-readable material lies in this portion of the description.

Such a description of the storage arrangement would define the device used as the transmittal medium, the storage density, and the parity of information on that device. Additionally, the number of files on the device, the record length, and the buffer size needed to read physical records from the device must be specified. The method of segmentation of the files into logical records must be described. The end of file recognition mark must be described.

The organization of the information provides the third element of the descriptive material. This should indicate the logical operations required to access each record on the data base, and the technique which must be used to go from one record to its logical successor. The organization of information can be as important as the content. The way in which data is stored contributes materially to the efficiency of the computations using that information. It also determines the number of applications to which that data can be put. Information which is organized in a distinctive manner is, for the purposes of computer processing, new information, even though the semantic content may be the same as another data base.

These three descriptive elements define a data base uniquely. If two products differ in any significant respects, then they are different products. What is a significant respect? To offer an example, data which was identical in every way except that the original was on a disc unit, and the alternate version was written on magnetic tape, would not be considered to differ in a significant way. In defining a significant respect, the desire is of least concern, and the semantic content the most. This term will be largely determined on a case-by-case basis. The purpose of this definition is to limit devious attempts to make copies not appear to

be copies. Some general guidance can be given in application of the term. The three descriptive elements defining a data base can be ranked in the order in which they are significant in differentiating data bases. This ordering is:

1. The semantic content of the data base.
2. The organization of the information.
3. The physical arrangement of the information.

The first and second defining elements would weigh heavily in differentiating data bases; the third element would be of limited application.

Given a way of uniquely specifying each information collection, we have established a pre-requisite for defining a protection system. That is, that each entity protected or contested can be described in unambiguous terms. While data can also be distinguished on a semantic basis alone, based on the subject class in which it falls--e.g. personal or technical--that distinction is not sufficient for our purpose. The category of personal data has been of great concern to civil-libertarians and we feel that the literature contains many valuable studies of precautions needed to protect the civil rights of the subjects of such information collections [16,108,109,110]. We will not discuss this problem particularly as this type of information of this nature ought to be treated

distinctly within a system which meets publicly known criteria for protection of individual rights. The recommendations of the Ware Commission under the auspices of the U.S. Department of Health, Education, and Welfare are exhaustive and we endorse them [94]. This commission recommends legislation which would establish a code of fair information practice for automated personal data systems. In particular, they recommend that safeguard requirements be defined for these data systems. They enumerate considerations for protection of data privacy and accuracy, and recommend a public notice requirement compelling such systems to reveal their existence and character. They establish a set of recommendations for statistical and research data systems which derive their information from personal data. In addition to other safeguards, they recommend that the raw data used for such work be made available so that the conclusions can be independently verified. These recommendations provide a framework for protection of individual privacy against both commercial interest such as credit bureaus and governmental data collection. We feel that data which falls under the scope of these recommendations ought to be specifically excluded from any other protective system, to avoid bypassing the deliberate protections established for civil rights.

Our concern is rather with protection for the commercial value of an information product. We propose a system which limits it concerns to the form and structure of material, and is not essentially interested in the content. Just as copyright may be used to protect a book which contains any kind of information, we wish our system to protect any material, but would exclude personal data for reasons of privacy.

The system which we propose should be consistent with the mandate of the Constitution concerning the protection of intellectual property. While the possibility may exist for a striking departure in the protection of such material, as some analyses of Goldstein [56] have indicated, we do not see the necessity or benefit for such a departure from traditional legislative behavior. We feel the protection that can be obtained in a traditional framework is satisfactory. Additionally, a particularly novel structure proposed for such a system would invite Constitutional challenge. The intent of proposing such a system would be to redress overlong neglect, and not to initiate complex litigation.

We feel that the philosophy which protects an implementation and not the underlying ideas is sound as a model for protection of computer data, and that, as

with the IBM proposal, such a structure ought to be designed with special attention to the particularities of the class of material protected. However, amending or modification of the copyright system in order to accomodate the information with which we are concerned would not be satisfactory. A new structure must be developed, although existing systems provide useful models. Enforcement of a system which includes injunctive relief, penalties, damages, and costs would be particularly useful.

We feel that there has been no evidence that the fundamental theorem on which our laws for protection of intellectual property are based--the Constitutional patent clause--is deficient in conception or operation. Therefore, that mandate ought to be adhered to in the development of additional structures to accomodate new technologies. We find no justification for any but a conservative approach. We need to bring a workable structure up to date, and do not find the necessity for violating the basic principles underlying systems of protection for intellectual property.

We propose a system for the registration of computer-based data. It would be most effective if this proposal could be combined with proposals of merit for protection of computer programs and enacted into

legislation. A definitive treatment of computer products would be a major contribution to the updating of our patent and copyright laws. Our particular proposal will be limited, however, to the protection of computer-based data. We find the IBM proposal for protection of programs attractive, and support their recommendation.

Our data protection system would be elective and would permit two levels of participation. One level would be full registration, which would require conformity to all the provisions of the system. The other level would be called "registration of interest" and would not afford any protection, but would rather provide a means of defining how a particular data system differed from fully-registered systems in order to avoid claims of infringement. Fraudulent registration in either category would, of course, not be upheld.

We feel that the registration system ought to cover the data portion alone of the data system which we recommended in our technical solution. The executive and transaction capabilities recommended can be protected in a system which is designed for programs. Since those elements may be used with a number of data bases in providing distinct data systems, we feel that the protection of such separable elements ought to be

performed by distinct means.

Additionally, a departure from precedent is evidenced in our proposal for compulsory licensing with the fees to be determined by the vendor, but challengable by the potential licensee. The precedent for compulsory licensing is found in the section of the Copyright Act which determines the conditions under which songs may be rendered into recordings*. That provision led to the creation of clearinghouses and complex methods for the collection and distribution of music royalties. We feel that there is justification for avoiding fixed license fees in the case of data, which varies widely in its cost and content. We provide for arbitration of challenged license fees to avoid the establishment of a quasi-monopoly through exorbitantly high royalties. The standards which would be used in such arbitration would be the actual cost of the data, the possible reasonable profit, and demand for the product, and other available economic information.

Machine use of material which previously had been copyrighted in human-readable form is a distinct possibility. As the hardware capacity of mass storage grows, the machine processing of full text becomes more

---

*Ch. 1, sec. 1 (e).

feasible. We feel that, when human-readable material protected by copyright is deliberately rendered into machine-readable form it ought to be mandatory that the proper compensation be paid to the copyright holder. This is accomplished in the copyright environment on behalf of composers whose songs are recorded. We feel that the analogy to machine input of text is compelling, and requires an equitable solution. This would require an amendment to the copyright act making such machine use specifically not an infringement if the proper royalties were paid. Such an amendment could be accomplished in an act creating the registration system. If it is desired to avoid the complexity of a text-processing clearinghouse then a lump-sum payment ought to be considered rather than use-by-use royalties. This would be practical in the case of computer data since the equipment required to utilize such material is substantial enough to limit the number of transfers of data. We propose a lump-sum royalty payment which would be equal to either one thousand dollars, or the licensing fee for the material for one occurrence of use for one month, whichever is the greater. This would be a sufficient amount to provide reasonable compensation to the copyright holder, but would not represent an unreasonable part of the machine-readable data base profits.

We propose the following to be considered as a model in developing legislation to protect computer data bases. Protection would be dependent upon conformity to the requirements specified, and neglect of any of the details could vitiate any protection.

1. The three descriptive elements which define an information collection and which must be supplied to the registry will be the narrative description of the subject matter, the description of the file and record structure, and the description of the organization of the data. Submitted material will be examined only for format, and not for correctness.

2. The narrative description of the subject matter and the description of the organization of the data will be published in a bulletin.

3. The description of the file and record structure, which will be sufficient to enable construction of the appropriate programs to read such information, will be kept secret for the term of the registration period.

4. A schedule of license fees will be deposited and may be obtained by the public upon request. If a potential licensee wishes to challenge this schedule, hearings will be held before the register to determine the fair schedule of fees.

5. A registration fee of ten dollars will be paid. If license fees are challenged before the register additional court costs may be assessed.

6. A statement of the use of any copyrighted material in the data base must accompany the deposit of required material. Failure to make such a statement will be grounds for a claim of infringement of copyright. Each publication of such a data base must be accompanied by payment of a royalty of

either one thousand dollars or one mont's license fee, whichever is greater. A publication shall be defined for this purpose as the conversion of the copyrighted material into a machine readable data base, no matter how many copies of the data base are subsequently released.

7. The registration of the data base may be challenged if the machine-readable product does not agree with the deposited narrative description or the description of file and record structure, or the description of the organization of the dta.

8. The proprietor will have the sole right to:

   a) Publish, copy, use, or vend a data collection which agrees with the deposited material which is required in section 1.

   b) Create alternate file and record structures for the material which meets the narrative description and data organization specifications required in section 1.

   c) Install a data base meeting the descriptive requirements of section 1 on any computer configuration.

9. Infringement will be defined as:

   a) Unauthorized creation of a machine-readable copy of a registered data base.

   b) Unauthorized access to or copying of any machine-readable storage or memory unit containing any files or records of a registered data base.

   c) Unauthorized conversion of any part of the registered data base into the internal machine representation of a computer for the purpose of being acted upon by a computer program.

d) Publication or use of a data base which has the same subject matter as required in the narrative description and the same file organization as the registered data base.

e) Unauthorized installation of the registered data base on any computer machinery.

10) The period of registration will be ten years and this registration will not be renewable. Registration will commence with the issuance of a certificate dated and stamped by the register upon receipt of the required deposit materials and the fee.

11) The registration level known as "registration of interest" shall convey none of the above benefits, but permits deposit with the registry a description of adata base showing how it differs from a registered data base. This form of registration shall be also valid for ten years. The deposited material may be obtained by the public upon request.

12) If any person shall infringe the sole rights reserved to the registrant, that person shall be liable:

a) To an injunction restraining such infringement;

b) To pay damages and the profits made from such an infringement;

c) Impoundment during action of all articles which allegedly infringe the registration;

d) Punishment by imprisonment of up to one year or a fine of not less than $1000 but not more than $10,000 or both;

e) Payment of full costs and attorney's fees.

Let us examine the proposal. The first item

defines the unique information collection by specifying the elements which must be described and deposited in order to identify it for registration. The publication of the material enumerated in the second item is for the purpose of obtaining that disclosure mandated in systems which protect intellectual property. The safeguarding of the material in item 3 is for the purpose of making access to the protected data difficult. Item 4 enumerates the means of compensation for use of such material, and makes licensing compulsory by requiring deposit of license fees.

The general intent of registration fees is to control the use of registration. For this reason, this proposal sets an arbitrarily low registration fee so that use will be wide. The provision for the handling of copyrighted material is for the purpose of ensuring equitable treatment of the copyright owner, and avoiding litigation if the proper course is followed.

The provision for challenge of registration defines broadly what may constitute fraudulent registration. A licensee who entered into a contract with a data base proprietor on the basis of the published material and found he was not receiving that data would be able to challenge the registration. Similarly, one who received a description of the file and record structure which

differed from the deposited description, or which was not sufficient for him to construct programs to use this machine-readable data could challenge the right of that proprietor to register such material.

Sole rights of the registrant include the right to install the data system on a machine, as well as customary rights to publish, use, copy, and sell the material. This right of installation is fundamentally the right to create a data system. Without the right to install the data base, there is no purpose to the creation of the executive and transaction capability of a data system. The inclusion of the exclusive right to implementation makes effective our technical proposal for protection. A data system may share its executive and transaction capability with other data bases belonging to that proprietor, but a competitor could not develop a new data system and use it to implement a system containing data which infringed on the protected data. The preceding right to create alternative file and record structures is based on the fact that implementation of a data base on different machines might result in different physical structures.

Infringement is defined in item nine. This definition differs slightly from that of sole rights granted to the proprietor since infringement covers

those actions which would interfere with the exclusive use of the data. Since the registration period is non-renewable, these rights are generous in the period which they cover. The motivation for making the registration non-renewable was the fast rate of change in the computing industry and the likelihood that a data base would be obsolete before it lost its registration.

The liabilities for infringement are traditional. The dollar value of the fines is set at a value which will be significantly high in view of the programs which can be made from computer materials. Similarly, the copyright royalties are sufficiently high to represent a significant control over the indiscriminate use o such material.

These recommendations are meant to constitute a protection system which is stringent enough to offer effective protection against misuse, but tailored to the specific material to be protected so that there will be no conflicts due to misinterpretation of requirements in the light of undefined technology. The actual drafting of legislation incorporating these proposals is a matter requiring particular skill and expertise in the legislative process. We do not possess this particular experience, and will not attempt to construct the wording of a model bill.

The question arises as to what jurisdiction should implement such a registration system. As we saw earlier, Goldstein stated that material not presently under the jurisdiction of the patent or copyright laws could be protected by the states [56]. However, information processing cannot be defined in terms of geographic jurisdictions. Communications channels and computer networks can span states, countries, and continents. The possibility of fifty distinct jurisdictions enacting different statutes for protection of such material is not appealing.

In addition to the enforcement problems, protection against infringement would be difficult if registration were only effective in one state. Permitting concurrent registration in a number of jurisdictions would not be feasible since there would be no practical way of determining whether these concurrent registrations were all the work of the proprietor, or were fraudulent registrations of infringing material. A potential data base creator would be placed under an extreme hardship if he had to search the registers of fifty different registries in order to ensure that his product did not infringe any existing data base. The arguments see compelling in favor of a single registry under Federal auspices.

We therefore recommend enactment of legislation in Congress which would implement our proposal for data protection, plus those meritorious proposals which may be at hand for protection of computer programs. We propose that this legislation amend the Copyright Act of 1909 to provide for the statutory payment of royalties for use of copyrighted material in machine-readable form, and so remove the possibility that such use would be generally considered an infringement. We feel that the mechanism of the proposed registration system offers the most equitable balance of the interests of proprietors and users, and that it can support and extend the technical safeguards which we have proposed above.

## VII. CONCLUSION

Computer-based data does not fit the traditional frame-work for protection of intellectual property. As we have seen, patent protection would be inappropriate, and the actual protection obtained under copyright registration is questionable because of precedents which distinguish between human and machine-readable material. While protection could be obtained under trade secret laws for such data which was not made publicly available, the growing interest in a marketable data base structure would preclude that form of protection from publicly available computer data. For such material as is not suitable for protection under trade secret laws, unfair competition laws have been used to obtain recourse for misuse. However, this is a dubious course, and cannot be greatly relied upon.

Therefore, we have proposed a structure for legal protection of computer-based data which is specifically iented to that material. We feel that a conservative approach to the design of such a system, using existing systems such as the copyright framework as a model is the most appropriate. The system which we propose is a registration system which is elective, and which grants the proprietor a monopoly for ten years over material which qualifies for protection.

This system is also accompanied by a proposal for technical protection of such material. The damage done by successful access to valuable data by an intruder is great enough that a technological barrier is required even though there may be possibilities of legal recourse. The theory that there must not have been unrestricted access to the material which was taken for the remedies to be applied may be applicable in such a case. These two structures--technical and legal--complement each other. While the technical barriers, no matter how effective, can be broken by sufficiently skilled and knowledgeable persons, they deter all intruders not in that class. The legal barriers provide redress and punishment in the event of such a successful intrusion. Thus, the development of a data product is susceptible only to risk commensurate to that of comparable products.

The present situation places an unacceptably high level of vulnerability on such data base products. While contractual specifications can be made defining precautions which must be taken, the expense and inconvenience of such precautions falls on the party who has the least to gain from that effort. The data proprietor is protecting his investment. The data user, who has entered into a contractual agreement to obtain the product at a certain cost, has far less interest in

the protection of the privacy of the product than the proprietor. For that reason, we have moved the actual responsibility for creation of the protective system to the data proprietor, and required in turn that the customer accept the product in its fully-secured form.

We realize that this fully-secured form places some burden on the user. However, this is far less than if he were required to implement protective mechanisms himself. The actions of the protective structure of the data system are restricted to the data system alone, with the exception that the operating system is required to interrogate file accesses to determine whether they request the area reserved for the data system. The executive and transaction capability which would be supplied with the data base would provide the capabilities which had been negotiated between the consumer and the proprietor, thus restricting him to those previously determined operations on the information. He would be unable to use his own code to implement any functions--whether agreed to or not. In addition, the use of the data system would be accompanied by record-keeping which was intended to further the integrity and safety of the product. This record-keeping would require that the users of the data base incur some overhead.

A major burden of such a system would be the liability which the user would incur should it be used improperly through his agency, or damaged through failure of the host environment. We consider the host computing environment potentially malicious and at best indifferent. We differ from conventional protection systems which attempt to define the class of users which have pre-defined rights to operate on data. We have only one user--the data system executive. This means that the interaction with the foreign environment is kept to a minimum.

The determined intrusion by a technically skilled and knowledgeable individual cannot be deterred by technological means. This type of misuse requires legal remedies since the data system represents an investment which must be protected. A skilled individual may violate the privacy and integrity of any data system. This must be dealt with administratively. Restricting the accessability of the technical information required to break into the system is an important element in protecting a computer-based system. The user should be required to create an administrative structure in which information concerning the data system is only supplied on a need-to-know basis. A system administrator could then be designated to have responsibility for maintenance of the integrity and privacy of the data

base and support systems.

The assignment of such responsibilities to the user is reasonable. Obtaining a valuable product or service implies that the user recognizes its value, and is in a position where he is obligated to maintain the confidentiality of any information which he has of that nature. He should not, and in our proposal is not, be responsible for actively implementing measures to protect the technical access to the data.

The record-keeping procedures of the executive would be alterable by a skilled intruder, but they would be hidden within the data system, and the need-to-know principle would effectively maintain the secrecy of the implementation of the audit and logs. It is also probable that the fact of alteration of those files would be obvious. Since the audit and logs are for the purpose of detection of suspicious accesses, they could be treated as write-only files, and unauthorized attempts to read them or backspace them could be summarily aborted. Similarly, the data organization on the audit and log files could be used to protect itself. Use of a redundant data entry structure, where changes must be internally consistent, would be one method of making unauthorized entries obvious. Since these files would be critical in legal proceedings involving

violation of registration rights, they ought to be treated with a high degree of caution.

Motivations for misuse of such systems would have to be strong since the legal structures provides for compulsory licensing at a fee which can be arbitrated. By making the legitimate access to registered material non-complicated, we correspondingly reduce the possibility for causal misaccess or snooping. The penalties are set sufficiently high that it is more reasonable to gain legitimate access than to attempt to misuse such data.

However, there will always exist some prospects of determined misuse. Competitive development of a similar product might be based on improper access to secrets embodied in the original. Espionage by industrial concerns in taking scientific or technical materials is not unheard of, nor is similar action by foreign countries. The technical defenses are intended to make the cost of such access prohibitively high in the information which required to carry it out.

The system which we propose balances the interests of the user and the vendor. The user acquires information which he considers of value without incurring the costs and effort of acquiring it and converting it to machine-readable form, maintenance of

changes, and development and testing of support software. The vendor retains control over the profitable elements of his product, which are its integrity and privacy. The user provides an appropriate host environment, and gains the ability to charge his use of the data internally, rather than incurring charges for out-of-house computer time, which would be in addition to his expenses for his in-house machine. The vendor in turn is relieved of the responsibility of hardware maintenance, and is not responsible for maintaining a production system on any machine.

The data base and executive would be registered under different protective systems, assuming that a parallel system is created for programs. If variations of a data base were created by the vendor which did not differ from each other in significant respects, they would be covered by the initial registration. If the final user was responsible for misuse of the data, the vendor would seek remedies under the registration system provisions.

Essentially what we have proposed is a new software industry. By providing a framework in which such a product would be viable, we have provided support for the initiation of marketing such material on a competitive basis. Given the real potential for

computing machinery which can support large data services, we have defined a legal structure in which such data services would obtain protection from misuse, and a technical protective scheme which would make it feasible to incorporate such data in an environment which is at best indifferent and at worst hostile. The two systems complement each other and strengthen the protection obtained alone from each. Thus, the rights and obligations of all persons involved in use of such material become defined, and the risks in such an industry are no more than in any comparable enterprise.

## REFERENCES


[1] Allen, Steven, et al. "New Technology and the Law of Copyright: Reprography and Computers," UCLA Law Rev. 15: April-Sept. 1968. 939-1028.

[2] Arnold, Tom and Goldstein, Jack. "Life Under Lear," Texas Law Rev. 48:(7) Nov. 1970. 1235-1260.

[3] Banzhaf, John F. III. "When a Computer Needs a Lawyer," Dickenson Law Rev. 71:(2) Winter 1967, 240-256.

[4] -----. "Copyright Protection for Computer Programs," The Law of Software, Washington: George Washington Univ., 1968, C33-C51.

[5] -----. "Computers and the Copyright Laws. A Commentary," Comm. ACM 10:(1) Jan. 1967, 61.

[6] Baran, Paul. "On Distributed Communications: Security, Secrecy and Tamper-Free Considerations," Security and Privacy in Computer Systems. ed. Lance J. Hoffman. Los Angeles: Melville Publ. Co., 1973, 99-123.

[7] Beardsley, Charles W. "Is Your Computer Insecure," IEEE Spectrum, Jan. 1972, 67-78.

[8] Bell, C.G. and Newell, A. Computer Structures: Readings and Examples. New York, McGraw-Hill, 1971.

[9] Bender, David. "Trade Secret Protection of Software," Software Protection by Trade Secret, Contract, Patent. Washington: Patent Resources Group, 1969.

[10] Benjamin, Curtis G. "Computers and Copyrights," Science 152: April 1966, 181-184.

[11] Bigelow, Robert P. (ed.) Computers and the Law. An Introductory Handbook. 2nd. ed. Chicago: Commerce Clearing House, Inc., 1969.

[12] Brandeis, Louis D. and Warren, Samuel J. "The Right to Privacy," Harvard Law Rev. 4:(5) 193 Dec. 15, 1890.

[13] Breyer, Stephen. "The Uneasy Case for Copyright: A Study of Copyright in Books, Photocopies and Computer Programs," Harvard Law Rev. 84:281-361. Dec. 1970.

[14] Burkhardt, Walter. Scrambling and Unscrambling Files for Security. PB-213-899, Springfield, Va: National Technical Information Service, Nov. 1972.

[15] Bush, George P. (ed.) Technology and Copyright. Mt. Airy, Md: Lomond Systems, Inc., 1972.

[16] Canada. Department of Communications/Department of Justice. Privacy and Computers. Ottawa. 1972.

[17] Carroll, J.M. and McLellan, P.M. "Fast 'Infinite-Key' Privacy Transformation for Resource-Sharing Systems," Proc. AFIPS Fall Joint Computer Conf. Montvale, N.J.: AFIPS Press, 1970, 223-230..

[18] Chastain, Dennis R. "Security vs. Performance," Datamation, Nov. 1973, 110-111, 116.

[19] CODASYL Systems Committee. Feature Analysis of Generalized Data Base Management Systems. New York: Association for Computing Machinery, May 1971.

[20] -----. CODASYL Data Base Task Group Report. New York: Association for Computing Machinery. April 1971.

[21] Conway, R.W. et al. "On the Implementation of Security Measures in Infomation Systems," Comm. ACM 15:(4) April 1972, 211-220.

[22] Cunningham, Dewey J. "Information Retrieval and the Copyright Law," Bull. Copyright Sc. 14: Oct. 1966, 22-27.

[23] Doerfer, G.L. "Limits on Trade Secret Law Imposed by Federal Patent and Antitrust Supremacy," Harvard Law Rev. 80: 1967 1432-1462.

[24] Falk, James W. "Copyright Infringement Problems," The Law of Software. Washington: George Washington Univ., 1969 A1-A14.

[25] Feinberg, Barry H. "The Viability of Trade Secret Protection after Lear v. Adkins," Villanova Law

Rev. 16:(3) March 1971 551-570.

[26] Ferrari, D. "Architecture and Instrumentation in a Modular Interactive System," Computer 6:(11) Nov. 1973, 25-29.

[27] Forman, Howard I. "The Changing Characteristics of Private Property," J. Pat. Off. Soc. 53:(18) Aug. 1971, 530-546.

[28] Foster, Caxtan C. Computer Architecture. New York: Van Nostrand Reinholt Co. 1970.

[29] Foster, Stanley H. "Comments on Painton and Company vs. Bourns, Inc.," J. Pat. Off. Soc. 53:(11) Jan. 1971, 732-742.

[30] Franklin, J. Thomas. "Proprietory Protection of Computer Data Bases," Computer Law Service 3: 1973, 4-4 Art. 3.

[31] Freed, Roy N. "Portection of Proprietory Software Programs in the United States." Typewritten Manuscript. 1971.

[32] Friedman, T.D. "The Authorization Problem in Shared Files," Security and Privacy in Computer Systems. ed. Lance J. Hoffman, Los Angeles: Melville Publ. Co., 1973, 159-185.

[33] Fromholz, Haley J. "Legal Protection of Proprietary Software," Computer 6:(12) Dec. 1973, 27-31.

[34] Galbi, Elmer W. "Copyright and Unfair Competition Law as Applied to the Protection of Computer Programming," Computer Law Service 3:1972, 4-3 Art. 1.

[35] -----. "Proposal for New Legislation to Protect Computer Programming," Bull. Copyright Soc. 17:(4) April, 1970 280-296.

[36] Garrison, W.A. et al. Privacy and Security in Banks. AD-718-406. Springfield, Va: National Technical Information Service Nov. 1970.

[37] Goldberg, David. "Legal Protection of EDP Software," Datamation May 1972, 64-70.

[38] Goldberg, Morton David. "Copyright for Computer Programs--Yes, But..." The Law of Software. Washington: George Washington Univ., 1969, B1-B40.

[39] Goldstein, Paul, "The Competitive Mandate: From Sears to Lear," J. Pat. Off. Soc. 53:(10) Oct. 1971, 627-668.

[40] Goldstein, Robert C. Position Paper on Computers, Data Banks, and the Bill of Rights AD-721-670. Springfield, Va: National Technical Information Service, 1971.

[41] Graham, G. Scott and Denning, P.J. "Protection--Principles and Practice." Proc. AFIPS Spring Joint Computer Conf. Montvale, NJ: AFIPS Press, 1972, 417-429.

[42] Graham, R.M. "Protection in an Information Processing Utility," Comm. ACM 11:(5) May 1968, 365-369.

[43] Greenbaum, Arthur J. "Copyright and the Computer," U.S. Congressional Record 114:(102) June 11-14 1968, 8-9.

[44] -----. "Computers, Coprights, and the Law Prior to Revision", Bull. Copyright Soc. 15:1967, 164-173.

[45] Greenberger, Martin (ed.) Computers, Communications and the Public Interest. Baltimore: Johns Hopkins Press, 1971.

[46] Hamilton, Peter. Computer Security. Philadelphia: Auerbach 1972.

[47] Hellman, J.J. Privacy and Information Systems: An Argument and an Implementation. AD-706-963. Springfield, Va: National Technical Information Service, May 1970.

[48] Hoffman, Lance J. and Miller, W.F. "Getting a Personal Dossier from a Statistical Data Bank," Security and Privacy in Computer Systems ed. Lance J. Hoffman, Los Angeles: Melville Publ. Co. 1973, 289-293.

[49] -----. "The Formulary Model for Flexible Privacy and Access Controls," Security and Privacy in Computer Systems ed. Lance J. Hoffman, Los Angeles: Melville Publ. Co., 1973.

[50] -----. "Computers and Privacy: A Survey," Computing Surveys 1:(2) June 1969, 85-103.

[51] Hollingworth, Dennis. "Enhancing Computer System Security," P-5064. Rand Corp. Santa Monica, Calif. Aug. 1973.

[52] Hopcroft, J.E. and Ullman, J.D. Formal Languages and their Relation to Automata. Reading, Mass: Addison-Wesley Publ. Co., 1969, 26-30.

[53] Kahn, David. The Codebreakers. New York: Macmillan Co., 1967.

[54] Kane, Danial H., Jr. "Limitations on the Law of Trade Secrets," J. Pat. Off. Soc. 53:(3) Mar. 1971 162-176.

[55] Kaplan, Benjamin. An Unhurried View of Copyright. Columbia Univ. Press, New York 1967.

[56] Kaul, Donald A. "And Now, State Protection of Intellectual Property?," American Bar Assoc. J. 60: Feb. 1974, 198-202.

[57] Lampson, Butler W. "A Note on the Confinement Problem," Comm. ACM 16:(10) Oct. 1973, 613-615.

[58] -----. "Dynamic Protection Structures." Proc. AFIPS Fall Joint Computer Conf. Montvale, NJ: AFIPS Press, 1969, 27-38.

[59] McCoy, G.T. "Rights in Data Clauses and their Impact on Information Functions of the Government," Computer Law Service 2: 1973, 3-6 Art. 2.

[60] McOustra, C.J.C. "Legal Protection for Computer Programs," The Computer Journal 8: Jan. 1966, 289-296.

[61] Milgrim, Roger M. "Sears to Lear and Painton," Harvard Law Rev. 84: 1970, 477.

[62] -----. "Sears to Lear and Painton: Of Whales and Other Matters," New York Univ. Law Rev. 46:(1) Mar. 1971, 17-34.

[63] -----. "Software, Carfare and Benson," Datamation. April 1973, 75-80.

[64] -----. "Trade Secret Protection and Licensing: A True Alternative," Bull. Am. Patent Law. Assoc. July 1972, 396-410.

[65] Miller, Arthur R. The Assualt on Privacy: Computers, Data Banks and Dossiers. Ann Arbor, Mich: Univ. of Michigan, 1971.

[66] -----. "The National Data Center and Personal Privacy," Security and Privacy in Computer Systems. Lance J. Hoffman, ed. Los Angeles: Melville Publ. Co., 1973, 21-30.

[67] Molho, Lee M. "Hardware Aspects of Secure Computing," Security and Privacy in Computing Systems. Lance J. Hoffman, ed. Los Angeles: Melville Publ. Co., 1973, 351-365.

[68] Morris, James H. Jr. "Protection in Programming Languages," Comm. ACM 16:(1) Jan. 1973, 15-21.

[69] Niblett, B.F. "Computers and Privacy," Privacy, Computrs and You. National Computing Centre, Manchester, UK 1972 17-23.

[70] -----. Digital Information and the Privacy Problem. Organization for Economic Co-Operation and Development. Paris. 1971.

[71] Nims, H.D. "Developments in the Law: Competitive Torts" Harvard Law Rev. 77: 1964, 888.

[72] Noll, A. Michael. "The Interactions of Computers and Privacy," Honeywell Computer J. 7:(3) 1973, 163-172.

[73] Orenbuch, Louis. "Trade Secrets and the Patent Laws," J. Pat. Off. Soc. 52:(10) Oct. 1970, 638-677.

[74] Parker, Donn E. et al. Computer Abuse. Menlo Park, CA: Stanford Research Inst. 1973.

[75] -----, and Nycum, Susan. "The New Criminal," Datamation Jan. 1974, 56-58.

[76] Palme, J. "Software Security." Datamation, Jan. 1974, 51-55.

[77] Patrick, R.L. "Privacy, People and Credit Services," Datamation, Jan. 1974, 48-50.

[78] Petersen, H.P. and Turn, R. "System Implications of Information Privacy," Proc. AFIPS Spring Joint Computer Conf., Montvale, NJ: AFIPS Press, 1967, 291-300.

[79] Reed, Irving S. "The Application of Information Theory to Privacy in Data Banks," R-1282-NSF Rand Corp, Santa Monica CA. n.d.

[80] Rossant, M.J. "The Phantom of Beverly Hills," Harpers 247, August 1973, 70-79.

[81] Saragovitz, Harry M. "Patents, Trade Secrets--Technical Data Use and Misuse by the U.S. Government," Computer Law Service 2: 1973. 3-6 Art. 3.

[82] Schroeder, M.D. and Saltzer, J.H. "A Hardware Architecture for Implementing Protection Rings," Comm. ACM 15:(3) March 1972, 157-170.

[83] -----. Co-operation of Mutually Suspicious Subsystems in a Computer Utility. AD-750-173. Springfield, VA: National Technical Information Service, Sept. 1972.

[94] Shannon, C.E. "Communication Theory of Secrecy Systems," Bell System Tech. J. 28:(4) Oct. 1949, 656-715.

[85] Sills, Arthur J. "Automated Data Processing and the Right to Privacy," Seton Hall Law Rev. 1:(1) Spring 1970 7-24.

[86] Skatrud, R.O. "A Consideration of the Application of Cryptographic Techniques to Data Processing," Proc. AFIPS Fall Joint Computer Conf. Montvale, NJ: AFIPS Press, 1969 111-117.

[87] Smith, L.D. Cryptography. The Science of Secret Writing. New York: Dover. 1955.

[88] Stahl, Fred. A. A Homophonic Cipher for Computational Cryptography. AD-758-317. Springfield, VA: National Technical Information Service, March 1973.

[89] Tasker, P.S. et al. Design and Certification Approach: Secure Communications Processor. AD-765-518. Springfield, VA: National Technical Information Service, June 1973.

[90] Titus, James P. "Copyrighting Computer Programs," Comm. ACM 9:(12) Dec. 1966, 879-880.

[91] Turn, Rein et al. "Privacy and Security in Databank Systems -- Measures of Effectiveness, Costs, and Protector-Intruder Interactions," Proc.

AFIPS Fall Joint Computer Conf. Montvale, NJ: AFIPS Press, 1972, 435-444.

[92] -----. Security of Computerized Information Systems. AD-709-366. Springfield, VA: National Technical Information Service, July 1970.

[93] U.S. Committee on Scientific and Technical Information. Legal Aspects of Computerized Information Systems. Washington,DC. Sept. 1972.

[94] U.S. Dept. Health, Education and Welfare. Records, Computers and the Rights of Citizens. Washington, DC July 1973.

[95] U.S. Congress. Committee on Government Operations. "Privacy and the National Data Bank Concept." 35th Rept. 90th Cong. 2nd. Sess. Aug. 1968.

[96] -----. "Retail Credit of Atlanta, Georgia," 90th Cong. 2nd Sess. May 1968.

[97] -----. "The Computer and Invasion of Privacy." 89th Cong., 2nd Sess., July 1966.

[98] U.S. Copyright Office. "Computer Programs. Circular 31D," Library of Congress. Washington, DC 1969.

[99] van Tassel, Dennie. "Cryptographic Techniques for Computers: Substitution Methods," Inform. Stor. Retr. 6: 241-249 (1969).

[100] -----. "Advanced Cryptographic Techniques for Computers," Comm ACM 12:(12) Dec. 1969, 664-665.

[101] Ware, Willis H. "Security and Privacy: Similarities and Differences," Proc. AFIPS Spring Joint Computer Conf. Montvale, NJ: AFIPS Press, 1967, 287-290.

[102] -----. "Security and Privacy in Computer Systems," Proc. AFIPS Spring Joint Computer Conf., Montvale, NJ: AFIPS Press, 1967, 279-282.

[103] Wegner, Peter. Programming Languages, Information Structures, and Machine Organization. New York: McGraw Hill, 1968.

[104] Weinstock, Charles B, A Survey of Protection Systems. AD-765-552, Springfield, Va: National Technical Information Service, July 1973.

[105] Weiss, Harold. "Computer Security: An Overview," Datamation. Jan. 1974. 42-47.

[106] Weissman, C. "Security Controls in the ADEPT-50 Time-Sharing System," Security and Privacy in Computer Systems. Lance J. Hoffman, ed. Los Angeles: Melville Publ. Co. 1973. 216-243.

[107] Wilkes, M.V. "On Preserving the Integrity of Data Bases," The Computer Journal 15:(2) Aug. 1972, 191-194.

[108] Westin, A.F. Privacy and Freedom. Atheneum. 1967. New York.

[109] -----. Information Technology in a Democracy. Cambridge, MA Harvard Univ. Press. 1971.

[110] ----- and Baker, Michael A. Databanks in a Free Society. New York: Quadrangle Books. 1972.

[111] Wollons, D.J. Introduction to Digital Computer Design. London. McGraw Hill Book Co. Ltd. 1972.

[112] Wydick, Richard C.. "Trade Secrets: Federal Preemption in Light of Goldstein and Kewanee," J. Pat. Off. Soc. 12:(55) Dec. 1973, 736-758.

## BIOGRAPHY

Margaret Corasick was born in Drexel Hill, Pennsylvania in 1942. She attended public schools there, and graduated from St. John's College in Annapolis, Maryland in 1964 with a BA. While working for the Western Electric Company at their Engineering Research Center in Princeton, New Jersey she started work on her master's degree at Drexel University. In 1966 she was transferred to Bell Telephone Laboratories in Murray Hill, New Jersey. She received her master's in Information Science in 1968. Currently she is a member of the technical staff at the Mitre Corporation in Bedford, Massachusetts.