Confidential Communications and Information in a Computer Era

John T. Soma

Lorna C. Youngs

Follow this and additional works at: http://scholarlycommons.law.hofstra.edu/hlr

Part of the Law Commons

Recommended Citation
Available at: http://scholarlycommons.law.hofstra.edu/hlr/vol12/iss4/2

This document is brought to you for free and open access by Scholarly Commons at Hofstra Law. It has been accepted for inclusion in Hofstra Law Review by an authorized administrator of Scholarly Commons at Hofstra Law. For more information, please contact lawcls@hofstra.edu.
CONFIDENTIAL COMMUNICATIONS AND INFORMATION IN A COMPUTER ERA

John T. Soma*
Lorna C. Youngs**

CONTENTS

I. INTRODUCTION ........................................ 850
II. TESTIMONIAL PRIVILEGES ........................... 852
    A. Attorney-Client Privilege ......................... 852
       1. Historical Development .......................... 852
       2. Elements of Attorney-Client Privilege .......... 853
       3. Attorney-Client Privilege in the Corporate Setting . 857
       4. The Effect of Data Processing on the Attorney-Client Privilege .... 860
          a. Reasonable Precautions ....................... 861
          b. Traditional Exceptions to the Nondisclosure to Third Parties Rule .... 862
          c. Agency ........................................ 864
          d. The Corporate Attorney-Client Privilege .... 866
          e. General Accessability of Files .......... 867
    B. Work Product Doctrine ............................ 869
    C. Other Testimonial Privileges .................... 872
       1. Accountant-Client ............................... 872
       2. Other Privileges ................................ 874
    D. Professional Responsibility and Computer Confidentiality ....... 875

* Associate Professor of Law, University of Denver College of Law; J.D., University of Illinois; M.A. in Economics, University of Illinois; Ph.D. in Economics, University of Illinois.
** Staff Attorney, Columbia Savings, a Federal Svgs. & Loan Assn., Denver, Colorado; B.S. 1972, Pennsylvania State University; J.D. 1983, University of Denver College of Law.
The authors wish to thank Paul J. Hemschoot, Jr., Vice President and General Counsel of Climax Molybdenum Company, a division of AMAX Inc., and his legal department for their support and encouragement in the writing of this article. The opinions expressed herein do not necessarily represent the opinions or views of AMAX Inc.

Published by Scholarly Commons at Hofstra Law, 1984
I. INTRODUCTION

With the increasing use of electronic word processing and computer technology to store information, the question arises as to whether the ease of accessibility of computer data bases, in either an authorized or unauthorized manner, acts as a de facto waiver of the privileged status of confidential information. The potential for problems in this area has increased with the expanding use of computers by the legal profession. Lawyers have discovered the increased efficiency of creating legal documents with word processors. Some courts have discovered that computers do a more efficient job of arranging court dockets,¹ and computer programs, such as LEXIS² and WESTLAW,³ have created huge legal data bases to assist in legal research. The acceptance of the computer in the legal world has been grudging but inexorable. Given the growing acceptance of computer technology in law offices, both law firms and corporate law departments must consider the ramifications of creating computer data bases that contain confidential information.

The types of confidential information that can be stored in computer data bases include communications occurring within the context of a special relationship, such as an attorney-client or physician-patient relationship, and thus protected by an evidentiary or testimonial privilege against disclosure, work product materials, and business information constituting trade secrets. Generally, in order to maintain an evidentiary privilege against the disclosure of confiden-

². See LEXIS Library Contents (March 1984).
tial information, the communication\(^4\) or, in the case of a trade secret, the information itself,\(^5\) must be cloaked in secrecy. The communication or information must remain confidential. In a noncomputer situation, this might involve maintaining a manual file system to which access is strictly monitored. The commingling of confidential and non-confidential documents might act as a waiver of the privilege and subject the confidential documents to legal discovery by opposing parties.\(^6\)

One could argue that a locked manual file system or safe can be broken into by a skilled burglar, just as a computer system can be accessed by an adept computer technician who can "unlock" the mathematical codes that protect the system. In reality, the computer system is no more accessible than the manual file. In fact, the computer system may be safer than a manual system because there are fewer individuals with the technical knowledge to break into a computer. Yet newspaper stories concerning the security problems of financial data bases highlight the problem of computer accessibility. Unlike breaking into a file room, accessing a data base to "steal" or change financial information is not always immediately discoverable, and the huge financial losses that can result might remain undetected until audits are conducted. Moreover, the increased attention given to the problems of computer security raises questions for courts considering the legal ramifications of storing confidential information on computer data bases.

This article analyzes the legal effects of placing privileged and confidential business information into computer data bases. Part II of this article explores whether evidentiary testimonial privileges are waived where unauthorized personnel may intentionally or inadvertently learn the contents of confidential documents stored in computerized data bases. This discussion is conducted from the perspective of law firms, which may utilize outside service organizations to maintain their computer equipment, and corporate legal departments, which may utilize the vast computer resources existing within the corporation. Part III of this article conducts a similar exploration with respect to the storage of confidential business information in computer data bases. Finally, part IV discusses recommendations and solutions for maintaining the confidentiality of computer stored information.

---

4. See infra notes 19-46 and accompanying text.
5. See infra notes 172-83 and accompanying text.
II. TESTIMONIAL PRIVILEGES

A. ATTORNEY-CLIENT PRIVILEGE

1. Historical Development.—The privilege of refusing to disclose information discussed between attorney and client is one of the oldest and most important of the testimonial privileges. In English jurisprudence, the rationale for the privilege was based on the concept of “honor among gentlemen,” a singular and peculiarly English notion that a gentleman’s sense of honor would compel him to keep secret that which had been told to him in confidence. Although the attorney was not compelled to disclose this confidence, the client could be compelled by a bill of discovery. In contrast, the rationale for the privilege in America has emphasized the need to encourage explicit and candid communications and full disclosure of all facts between the attorney and client, to enable the attorney to fulfill the duty of providing the client with the best representation possible.

The theory underlying the attorney-client privilege is that proper representation outweighs the possible harm that may arise from suppressing evidence. The opponents of a strong attorney-cli-

7. Id. § 207, at 504-05.
8. Id. at 505. See generally 8 J. Wigmore, EVIDENCE § 2286 (McNaughton rev. 1961).
Aside from the pragmatic approach to the privilege, the importance of this doctrine has been emphasized in the developing area of privacy law regarding the right to be left alone in certain special communicative relations. This concern was recognized by the Seventh Circuit Court of Appeals when it stated that “[t]he basis for the privilege is to afford the client a reasonable expectation of privacy and confidentiality with regard to disclosures made during the course of consultation with his attorney.” In re January 1976 Grand Jury, 534 F.2d 719, 728 (7th Cir. 1976) (emphasis added). Finally, it has been suggested that it is fundamentally unfair to force an attorney to disclose damaging admissions made to him by his client. See generally Louisell, Confidentiality, Conformity and Confusion: Privileges in Federal Court Today, 31 Tul. L. Rev. 101, 111 (1956).
9. 6 MODEL CODE OF EVIDENCE 146 (1942).
11. 6 MODEL CODE OF EVIDENCE, supra note 9, at 147.

This rationale has been long recognized by the U.S. Supreme Court which stated that the privilege “is founded upon the necessity, in the interest and administration of justice, of the aid of persons having knowledge of the law and skilled in its practice, which assistance can only be safely and readily availed of when free from the consequences or the apprehension of disclosure.” Hunt v. Blackburn, 128 U.S. 464, 470 (1888). The purpose of the privilege “is to encourage full and frank communication between attorneys and their clients and thereby promote broader public interests in the observance of law and administration of justice.” Upjohn Co. v. United States, 449 U.S. 383, 389 (1981). “The lawyer-client privilege rests on the need for the advocate and counselor to know all that relates to the client’s reasons for seeking representation if the professional mission is to be carried out.” Trammel v. United States, 445 U.S. 40, 51 (1980). It is interesting to note that European observers believe that the privilege aids
ent privilege, however, complain that nondisclosure is the antithesis of an inquiry into the truth. The United States Supreme Court has recognized the suppressive effect of the privilege and has limited the privilege to protect only those communications that might not have been made absent the privilege, and which are necessary to obtain informed legal advice.

2. Elements of Attorney-Client Privilege.—According to Dean Wigmore’s treatise on evidence, the following elements comprise the attorney-client privilege:

(1) Where legal advice of any kind is sought, (2) from a professional legal adviser in his capacity as such, (3) the communication relating to that purpose, (4) made in confidence, (5) by the client, (6) are at his instance permanently protected, (7) from disclosure by himself or by the legal adviser, (8) except the protection be waived.

Courts have generally placed the burden of establishing these elements upon the party asserting the privilege.

It is important to note that the privilege protects only the communications between attorney and client for the purpose of obtaining legal advice, not the information contained in the communications. If the information discussed between the attorney and client is available from other sources, it will be discoverable from those sources. Therefore, a basic premise of this article will be that storing communications in computer data bases does not broaden or enlarge the attorney-client privilege, because the information in the data base is still discoverable from other sources. It is thus suggested that in determining attorney-client privilege claims, computer data bases be treated in the same way as a manual file system.

As noted above, in order for the attorney-client privilege to ex-

---

2. See id.; see also 2 D. LOUISELL & C. MUELLER, FEDERAL EVIDENCE § 207, at 508 (1978).
7. See id.; see also 2 D. LOUISELL & C. MUELLER, FEDERAL EVIDENCE § 209, at 528 (1978).
tend to attorney-client communications, the statements must be made in confidence. The term “confidence” requires that the communications have not been disclosed to others, and whether a particular communication is confidential depends largely on the circumstances. It has been suggested, for example, that the presence of a third party who overhears the communication destroys the privilege because such a circumstance indicates that the communication was never intended to be confidential. In addition, subsequent acts by the client, such as voluntary disclosure of the communications, may act as a waiver of the confidentiality. Some authorities hold that waiver of confidentiality must be made voluntarily. There is disturbing authority, however, that argues that even involuntary disclosures can defeat the privilege.

Under the involuntary disclosure theory, even an eavesdropper who surreptitiously hears the communication is not precluded from testifying as to what he overheard. Indeed, according to Dean Wigmore’s treatise on evidence, involuntary disclosures of privileged information, such as those resulting from theft or loss, are not protected. Under the Wigmore approach, even though the client and attorney are immune from being compelled to disclose privileged matter, the client assumes the risk that some third party might obtain knowledge of the privileged communication and reveal what he learns. Wigmore opines that this theory applies equally to stolen privileged documents and to surreptitiously overheard privileged conversations.

18. See supra note 14 and accompanying text.
19. 8 J. Wigmore, supra note 8, § 2311, at 599.
20. Id. at 600.
21. Id. at 601-03.
24. 8 J. Wigmore, supra note 8, § 2325.
25. Id. See also 81 Am. Jur. 2d Witnesses § 187 (1976).
27. Id.
28. Id. In the criminal setting, the sixth amendment often serves to shield the attorney-client privilege from intrusion by the state. See Henry v. Perrin, 609 F.2d 1010 (1st Cir. 1979), in which a proposed prison guard inspection of an attorney’s papers for textual contraband was held to have infringed upon the inmate’s sixth amendment right to counsel because “important and privileged information in a lawyer’s file is vulnerable to disclosure, or at least that the fear of meaningful disclosure is reasonable, by even a brief spot viewing of each page.” 609 F.2d at 1013. The court remanded the case to the district court to hear evidence on
It appears, however, that the modern trend is away from Wigmore's approach and toward a standard under which the privilege will not be lost if the attorney and client take reasonable precautions to ensure confidentiality, but are, nonetheless, overheard by a surreptitious eavesdropper. In the case of In re Grand Jury Proceedings Involving Berkley and Co., the federal district court, while initially following the Wigmore approach, subsequently reversed itself on rehearing in light of what it termed the modern trend toward acceptance of the reasonable precautions standard. In Berkley, a former corporate employee had taken the corporation's documents and disclosed them to the government. After noting that the employee was not authorized to retain the subject documents, the court stated that "to the extent the documents can be viewed as stolen, following the modern trend [the documents] should not lose the protection of the privilege." Moreover, the court analogized the employee's unauthorized disclosure of documents to an attorney's bad faith disclosure of client confidences without the client's approval and against the client's interest; the court noted that in that situation, even Wigmore would sustain the privilege claim. The court therefore concluded that "modern precedent would seem to suggest that the documents disclosed by [the employee] should not lose their privileged status simply because of the manner in which they were disclosed." The Federal Rules of Evidence implicitly rejected Wigmore's harsh approach to the privilege. As originally drafted, Article V contained thirteen rules defining nonconstitutional privileges that the federal courts should recognize, including, inter alia, lawyer-client, husband-wife, religious, psychotherapist-patient, trade secrets, and informer identity privileges. Under proposed Rule 511, no privilege

31. Id. at 869. The court cited 2 J. Weinstein & M. Berger, supra note 29, for support of this "modern trend." Id.
32. 466 F. Supp. at 869.
33. Id.
34. Id.
35. Id.
36. Id.
would be waived unless the holder of the privilege voluntarily disclosed his communication. Proposed Rule 503, setting forth the attorney-client privilege, defined a confidential communication as one “not intended to be disclosed to third persons other than those to whom disclosure is in furtherance of the rendition of professional legal services to the client or those reasonably necessary for the transmission of the communication.” Although Congress chose to implement only Rule 501, which left privileges to be developed by federal courts on a case-by-case basis, several states have enacted the proposed rules with these requirements and definitions substantially intact.

Even under Wigmore’s analysis, there have always been important limitations on the general rule that disclosure to a third party waives the privilege. The confidential nature of a communication may be recognized despite the presence of a third party where the third party is the confidential agent of either the client or the attorney, such as a language interpreter. This principle extends to other experts and assistants who may be necessary to enable the lawyer to understand certain aspects of the client’s case, such as accountants, psychiatrists and scientists. Justice Traynor has stated, for exam-

38. Id. 511, 56 F.R.D. at 258. 
39. Id. 503, 56 F.R.D. at 236 (emphasis added). The Supreme Court Standard 503 allowed the attorney-client privilege to be asserted to prevent anyone from testifying as to a confidential communication. 503(b), 56 F.R.D. at 236. This standard, as enacted by the New Mexico legislature states: “A client has a privilege to refuse to disclose and to prevent any other person from disclosing confidential communications made for the purpose of facilitating the rendition of professional legal services to the client . . . .” N.M. STAT. ANN. § 20-4-503 (Supp. 1975) (emphasis added). Under Supreme Court Standard 503, confidentiality is defined in terms of intent. Where the circumstances indicate an intent to keep a communication undisclosed, the communication is confidential. Taking or failing to take precautions will have bearing on intent. 2 J. WEINSTEIN & M. BERGER, supra note 27, § 503, at 5.


42. Id. § 209, at 529-30.
ple, that:

when communication by a client to his attorney regarding his physical or mental condition requires the assistance of a physician to interpret the client’s condition to the attorney, the client may submit to an examination by the physician without fear that the latter will be compelled to reveal the information disclosed.43

Similarly, the attorney’s employees or “functionaries,” such as secretaries, clerks, office managers, messengers, switchboard operators, and paralegals, have all been viewed as extensions of the attorney for the purpose of analyzing the privilege.44 In United States v. Kovel,45 for example, the court stated that “the complexities of modern existence prevent attorneys from effectively handling clients’ affairs without the help of others; few lawyers could now practice without the assistance of secretaries, file clerks, telephone operators, messengers, clerks not yet admitted to the bar, and aides of other sorts.”46

The attorney-client privilege is meant to protect confidential communications between the attorney and his client. Although there is some dispute among authorities as to exactly what constitutes disclosure to a third party, all are in agreement that limited disclosure to certain authorized personnel will not destroy the privilege.

3. Attorney-Client Privilege in the Corporate Setting.—Although the attorney-client privilege has been extended to corporations,47 courts have grappled with defining precisely which corporate employees constitute the client.48 Since the privilege extends only to confidential communications between the client and at-

43. San Francisco v. Superior Court of San Francisco, 37 Cal. 2d 227, 237, 231 P.2d 26, 31 (1951) (citations omitted). This situation is to be distinguished from one in which an expert is retained with the expectation of being called as a witness that would be subject to discovery. Here, the expert acts as an intermediary, facilitating the communication between attorney and client, rather than simply testifying in his own behalf as an expert to support the client’s position.
44. 2 D. LOUISELL & C. MUELLER, supra note 6, § 209, at 530-31. “Where such persons overhear communications between lawyer and client, either because their assistance is needed in conjunction [sic] with supplying legal representation or because they eavesdrop or accidentally overhear or see communications between lawyer and client, the privilege is not destroyed.” Id. at 532.
45. 296 F.2d 918 (2d Cir. 1961).
46. Id. at 921.
48. See infra notes 49-71 and accompanying text.
torney and a limited group of third parties,\textsuperscript{49} determining who should be considered the corporate "client" is critical to privilege claims.

The first attempt to define the client, often referred to as the "control group" approach,\textsuperscript{50} was enunciated in \textit{City of Philadelphia v. Westinghouse Electric Corp.}\textsuperscript{51} In \textit{Westinghouse}, the district court stated that the privilege applied only to a corporate employee who was "in a position to control or even to take a substantial part in a decision about any action which the corporation may take upon the advice of the attorney," or who was "an authorized member of a body or group which has that authority."\textsuperscript{52} In contrast, the United States Court of Appeals in \textit{Harper & Row Publishers, Inc. v. Decker}\textsuperscript{53} focused on the nature of the matter being communicated,\textsuperscript{54} an approach often known as "the scope of employment" concept.\textsuperscript{55} According to \textit{Decker}, in order for the privilege to be applicable the employee seeking protection must have made the communication at the behest of a superior; the subject matter of the problem on which legal advice was to be rendered had to be within the scope of the employee's corporate duties; and the subject matter of the communication must have been within the employee's performance of his corporate duties.\textsuperscript{56}

Finally, in \textit{Upjohn Co. v. United States},\textsuperscript{57} the Supreme Court rejected the "control group" test as too narrow.\textsuperscript{58} In \textit{Upjohn}, the corporation's general counsel was informed that certain payments may have been made by one of the corporation's foreign subsidiaries to foreign government officials, a possible violation of the Foreign Corrupt Practices Act.\textsuperscript{59} Counsel, therefore, began an internal investigation, interviewing corporate employees and officers and sending ques-
tionnaires concerning the details of the alleged payments to foreign managers. The Internal Revenue Service ("IRS") subsequently demanded production of the questionnaires and the general counsel's notes of his interviews. The corporation declined to produce these documents, arguing that the material was protected by the attorney-client privilege and also constituted work product prepared in anticipation of litigation.

The Court of Appeals for the Sixth Circuit held that the attorney-client privilege did not apply to communications that were made by a corporation's officers or agents who were not part of the "control group," and that the work product doctrine did not apply to an IRS summons. The Supreme Court reversed, reasoning that the control group test did not account for the fact that the privilege protects "not only the giving of professional advice to those who can act on it but also the giving of information to the lawyer to enable him to give sound and informed advice." The Court noted that the middle and lower level employees, who were not in control of the corporation's response to legal advice, were the very individuals who had the relevant information needed by the corporation's attorney. If lower echelon employees were not covered by the attorney-client privilege, the very purpose of the privilege would be frustrated by discouraging the communication of information to the attorney who must advise the corporate client. The Court noted, moreover, that a proper privilege should be sufficiently clear for lawyers to rely upon, and therefore rejected the control group test because it produced divergent court decisions as to which officers actually constituted the control group.

Chief Justice Burger, concurring in part, stated that the Court should have offered a more precise rule: namely that "a communication [be] privileged . . . when . . . an employee or former employee speaks at the direction of the management with an attorney regarding conduct or proposed conduct within the scope of employment."

60. Id.
61. Id. at 387-88.
62. Id. at 388.
63. United States v. Upjohn Co., 600 F.2d 1223, 1225 (6th Cir. 1979).
64. Id. at 1228 n.13.
65. 449 U.S. at 390 (citations omitted).
66. Id. at 391.
67. Id. at 392.
68. Id. at 393.
69. Id. at 403.
The Court decided the case on its facts, however, and chose not to formulate such a general rule. As a result, it is unknown whether the Court would apply the scope of employment test in a different factual setting.\textsuperscript{70}

Computer programmers and other computer service providers are unlikely to be considered "clients" under any of these approaches to the attorney-client privilege. Since the computer personnel will generally program the computer with information received from others, corporate counsel would be unlikely to seek substantive information from them, obviating the need for a privilege. The transfer of client communications to data processing personnel, however, may be significant, since it appears that in order for communications to be protected by the privilege, those communications must be cloaked in some degree of confidentiality.\textsuperscript{71} Thus, the \textit{Upjohn} case remains relevant to the inquiry into the effects of data processing on the attorney-client privilege.

4. \textbf{The Effect of Data Processing on the Attorney-Client Privilege.}—The use of word processing and other computer technology in the preparation, storage and communication of client materials requires the involvement of third party computer technicians and service personnel. Such personnel may be employees of the client, as in the case of an in-house law department with a data processing staff; persons under contract with the law firm or corporation, as in timesharing arrangements; or persons even more remotely connected to the work, such as outside maintenance vendors. Any of these personnel may obtain access to confidential client communications in the course of their ordinary duties or as a result of an unauthorized search of the files.\textsuperscript{72} In this regard, data processing personnel may be analogous to the eavesdropper or innocent overhearer.

As previously noted, Wigmore's treatise suggests that if a third party overhears or steals the contents of attorney-client communication, that third party may testify as to what he or she learned.\textsuperscript{73} Thus, it is conceivable that computer technicians who obtain access

\textsuperscript{70} See 2 J. \textsc{Weinstein} \& M. \textsc{Berger}, \textsc{Weinstein's Evidence} \textsection 503(b)(04), at 503-55 (1982).

\textsuperscript{71} See infra notes 98-101 and accompanying text.

\textsuperscript{72} Sabotage and theft of information by malcontent employees is occurring. See generally Espionage in the Computer Business, \textit{Bus. W.}, July 28, 1975, at 60; Hoyt, \textit{The Computer as a Target for Industrial Spy}, 1 \textsc{Assets Protection} 41 (Spring 1975). Financial institutions are the most obvious targets of the computer criminal. See Sokoli\textsc{k, Computer Crime - The Need for Deterrent Legislation}, 2 \textsc{Computer L.J.} 353 (1980).

\textsuperscript{73} See supra note 26 and accompanying text.
to confidential communications may be free to testify regarding the communication they obtained. There are, however, several theories to prevent such a result.

As already noted, for example, the modern trend appears to be toward a "reasonable precautions" standard. In addition, there are several important limitations upon the general rule that disclosure to third parties constitutes a waiver of the privilege. One key focus of the analysis must be to determine whether data processing personnel are analogous to any of the other third party exceptions that have been carved out by the courts: experts who facilitate attorney-client communications; functionaries who are necessary to the communication; or confidential agents who are under a duty to maintain the confidentiality of the disclosures made by the principal. In short, adequate theories exist to afford increased coverage of the attorney-client privilege for data processing personnel. The advantages and drawbacks of each of these approaches will be analyzed below.

a. Reasonable Precautions.—The modern trend is toward protecting the attorney-client privilege if reasonable precautions have been taken to prevent loss of the confidentiality of the communications. Unlike the Wigmore analysis, this theory does not hold the client strictly liable for disclosures, but, instead, adopts an approach similar to negligence.

There are problems, of course, with utilizing any standard based on reasonableness. Foremost is the difficulty of developing a clear test on anything but a case-by-case basis. Reasonableness as a concept permeates the Uniform Commercial Code for the purpose of facilitating day-to-day business operations. A similar approach could be implemented for determining the prudent use of the computer by the legal practitioner. Although the reasonable person standard has worked well in negligence theory, its use in the computer

---

74. See supra note 29 and accompanying text.
76. Id. at 530-31.
77. Id.
78. See supra note 29 and accompanying text.
79. 8 J. WIGMORE, EVIDENCE § 2325 (McNaughton rev. 1961).
80. The United States Supreme Court, in Upjohn Co. v. United States, specifically emphasized the need for clarity in defining the attorney-client privilege. 449 U.S. 383, 392-93 (1981). For a further discussion of Upjohn, see supra notes 55-67 and accompanying text.
81. U.C.C. 2-205 (reasonable as to time); 2-302 (reasonable opportunity to present evidence); 2-606 (reasonable opportunity to inspect); 2-706 (reasonable manner for resale); 9-207 (reasonable care of collateral); 9-504 (reasonable preparation or processing of collateral); 9-507 (sale in commerically reasonable manner) (1981).
context requires a certain amount of technical sophistication on the part of the client that is probably unrealistic. In a non-computer world it may be entirely reasonable to expect the client simply to assure himself that he and his attorney are alone in the office, or to presume that a file room in which any written client communications are kept is locked. It is, however, beyond the capacity of most clients to inquire as to what steps are being taken to preserve the confidentiality of computer files, even assuming that the client is aware that the attorney has a computer file system. Requiring certain “reasonable precautions” in utilizing computers might also have ramifications on the attorney's duty not to disclose client secrets and confidential communications, which should not be lightly ignored by the attorney establishing a law office for the twenty-first century. The imprecision with which these precautions are defined may “chill” communications if computers become readily used to store sensitive materials.

Notwithstanding these problems, the “reasonable precautions” approach provides a basis for protecting the attorney-client privilege where data processing personnel are involved. Under this approach, the attorney, rather than the client, is likely to be primarily responsible for assuring that reasonable precautions are taken; the attorney, of course, is in a better position to control the data processing persons' use of sensitive files. The client should reasonably expect that his attorney will exercise adequate care to protect the confidential communications from unnecessary disclosure. In fact, lawyers have ethical obligations to exercise due care in maintaining their clients' confidences. In part III of this article, specific recommendations are offered to guide lawyers in assuring that adequate care is taken with respect to storing confidential materials in computers.

b. Traditional Exceptions to the Non-Disclosure to Third Parties Rule.—Whether data processing personnel can be brought within the attorney-client privilege as experts who facilitate attorney-client communications, or as functionaries, is not free from doubt. Yet, classifying them as such would eliminate the uncertainty inherent in the reasonable precautions approach.

It is unlikely that data processing personnel would be classified as “experts” facilitating attorney-client communications. Experts are typically those who actually assist the lawyers in understanding or

82. See infra notes 96-104 and accompanying text.
83. Model Code of Professional Responsibility EC 4-3 (1980); see infra notes 154-64 and accompanying text.
formulating their clients' cases, such as doctors or accountants. In contrast, data processing personnel merely assist after the communications between lawyer and client have occurred. Computer personnel do not facilitate the actual communication or assist in analysis, but merely assist in the ultimate memorialization of the communications.

Data processing personnel are more appropriately covered by the functionary exception. In order to come within the parameters of this exception, a person must generally assist the attorney in effectively handling his clients' affairs. Data processing personnel fit nicely into this category. Furthermore, this exception offers clear guidelines for both the attorney and the client and would be unlikely to have a chilling effect on communications as would the reasonable precautions standard.

Differences between the functions performed by traditional functionaries such as legal secretaries, and those performed by data processing personnel, create some risk that courts will refuse to classify computer employees under the functionary exception. The secretary or clerk acts within a zone of confidentiality in which there is an expectation that, because of the clerk's intimate involvement in the communication, privacy or secrecy will be maintained. In contrast, the main function of data processing personnel is operating and maintaining the computer hardware and software; they are not generally concerned with the actual contents of the data base except for storage purposes. In the course of their maintenance, however, data processing people must have access to data bases, permitting them to search for and read documents that a secretary, clerk, or other mere computer "user" might be unable to access because of a security system permitting access only through the use of special codes. It is unlikely that a data processing organization could function effectively if it were not authorized to access certain information or data bases. More importantly, it would be practically impossible to actually deny access to certain files when skilled computer technicians have the ability to juggle the codes and gain access.

Although data processing personnel can thus be distinguished

84. See supra text accompanying note 42.
85. See supra notes 44-46 and accompanying text.
86. Id.
87. For a discussion of the reasonable precautions standard and its chilling effect, see supra notes 78-82 and accompanying text.
88. See infra notes 189-99 and accompanying text.
from the secretary, file clerk, or telephone operator, the similarities among all of these personnel are far more important with respect to the issue of attorney-client privilege than are the differences. All perform routine tasks, during the course of which some or all of a communication may be overheard or read. Unfortunately, regardless of how ideally suited the functionary exception may be, the issue simply has not yet surfaced in any reported cases. Since many courts believe that privileges work in derogation of the search for truth, they may be reluctant to extend this exception to data processing personnel.89

c. Agency.—Agency concepts may also provide a theory to afford protection to attorney-client communications that are accessible to data processing persons. Agency is a fiduciary relationship whereby one party consents to have another party act on its behalf and subject to its control.90 Generally, the relationship of principal and agent is created by agreement.91 An agent can be appointed to do the same acts and to achieve the same legal consequences as its principal could have performed or achieved, unless the agreement violates public policy or the conduct to be performed is criminal or tortious.92 Agency concepts are particularly relevant to this inquiry because agents are subject to an obligation of confidentiality apart from the attorney-client setting: An agent is under a duty not to furnish to others, or to use itself, either for the purpose of acquiring property or doing any other act in opposition to the principal’s interest, any information given to the agent in confidence by the principal or acquired by the agent in the course of, or on account of, the agency.93

In the case of an in-house corporate legal department where the data processing personnel are employees of the corporation, it can be readily argued that such personnel are either agents of the corporation—“the client”—or of the legal department—“the attorney.” These personnel assist corporate attorneys in storing communications between those attorneys and the corporation and are often required to sign employment agreements that may be found to invoke the con-

90. 3 Am. Jur. 2d Agency §§ 1, 17 (1962).
91. Id. at § 17.
92. Id. at § 20.
93. Id. at § 225.
fidentiality obligations of an agent. Moreover, at least in the area of tort liability, such persons are often found to be the agents of the corporation.\textsuperscript{94} Similarly, data processors working for a law firm may also be viewed as agents of the attorney. They certainly are subject to the management and control of the managing partners, at a minimum, and may be subject to the actual control of the lawyer on the case.

Of course, from a strict standpoint, it would probably have to be argued that the relationships involve implied agency. This is especially true with respect to outside service organizations, such as maintenance vendors and timesharing operators, who are one step further removed from the attorney-client relationship than is the in-house data processing department. Law firms and business enterprises that are too small to have their own data processing departments often utilize computer timesharing agreements in which various customers utilize the computer systems of a company from their own place of business through the use of telephone facilities.\textsuperscript{95} Confidentiality of attorney-client communications is required, of course, in both the timesharing arrangement and the service organization’s computer maintenance agreement with a law firm or other business. The question becomes whether the outside service organization or timesharing business can be construed as the agent of the law firm or corporate legal department for the limited purpose of maintaining the confidentiality and secrets contained on computer data bases. In

\textsuperscript{94} Restatement (Second) of Agency §§ 216, 217A (1958).

\textsuperscript{95} Even companies involved in the business of selling computer time may face problems in maintaining the confidentiality of their computer-stored data. In the case of Com. Share, Inc. v. Computer Complex, Inc., two companies were involved in the business of selling computer time on a “time sharing” basis where customers could use the computer system concurrently and pay only for the actual time they used the computer system. The companies had entered into a “Technical Exchange Agreement” where the “plaintiff supplied to defendant, in confidence, information, training, know how, documents, tapes, tangible things and other technology developed by plaintiff.” 338 F. Supp. 1229, 1231 (E.D. Mich.), aff’d, 48 F.2d 134 (6th Cir. 1972). The agreement specified that the parties “agreed not to lease, sell or otherwise divulge to any third party interest, without the prior written consent of the other, any and all systems software developments supplied to it by the other.” Id. at 1232. The parties terminated the agreement after three and one half years by mutual agreement. Nine months later, the defendant announced plans to sell substantially all of its assets and goodwill related to its computer time sharing operations to a third party who was a competitor of the plaintiff. Id. The plaintiff then filed a motion for preliminary and permanent equitable relief. Id. Noting, \textit{inter alia}, the use of notices in the software and the use of passwords, the court found that “the utmost caution was used by plaintiff in protecting the secrecy of this software.” Consequently, the court granted the motion for equitable relief and protected the information against disclosure. Id. at 1234.
the current evolutionary state of maintenance and time-sharing contracts, it is unclear whether an express agency relationship will exist, especially with regard to the narrow issue of confidentiality.

In addition, the outside service organization or timesharing business may contract with an enterprise to maintain the enterprise’s own computer equipment or to afford the enterprise computer time to process its business data. Although such a service organization may be viewed as an independent contractor rather than an agent because the service organization is not controlled by the person with whom it contracts, independent contractors have been classified as agents. The best view is that, by exchanging obligations of confidentiality as to the proprietary and confidential information each contractual party may be exposed to, a fiduciary relationship is created between the parties for the limited purposes of ensuring the confidentiality of this information.

d. The Corporate Attorney-Client Privilege.—In the corporate context, it could be argued that communications between corporate counsel and corporate employees should lose their otherwise privileged status because data processing personnel have access to these communications. However, under the approach suggested by Judge Weinstein’s treatise on evidence, one of the relevant factors to consider is whether access to the attorney-client communications was limited solely to those employees who needed to know the contents of the communications. Although the Supreme Court did not explicitly adopt this standard in *Upjohn Co. v. United States*, the Court did note that “[p]ursuant to explicit instructions . . . the communications were considered ‘highly confidential’ when made, . . . and have been kept confidential by the company.”

Utilizing this “need to know” theory, those seeking to assert the privilege may argue that the involvement of data processing personnel in the transmission of communications by computer, the storage of such information, and the maintenance of both hardware and software systems requires that such personnel know a limited amount of confidential information within the scope of their employ-

96. See Restatement (Second) of Agency § 2(3) (1958).
97. Id. See also 41 Am. Jur. 2d Independent Contractors § 3 (1968).
100. Id. at 395 (footnote and citations omitted).
ment. In diagnosing system malfunctions, technicians may have to access the confidential file in which the malfunction occurred. Additionally, in order to protect against accidental or purposeful destruction of files, both confidential and ordinary files must be copied and stored. In each of these instances, data processing people have the potential for purposefully or inadvertently reading confidential files. Although the data processor merely requires access to the file, and not necessarily knowledge of its contents, such access should be sufficient to meet the "need to know" standard. If the communication is otherwise cloaked in secrecy, as the Court noted was done in *Upjohn*, the communication should not lose its privileged status merely because computer workers may have access to it.

**e. General Accessibility of Files.**—An issue related to a computer employee's access to confidential information is whether the failure to segregate confidential files, either apart from the computer files, or in a separate file, is itself a waiver of the privilege.

Although there is little authority on the issue, one federal district court, in *James Julian, Inc. v. Raytheon Co.*, held that certain privileged memoranda written by corporate counsel did not lose their confidential status because they were placed in a general corporate file. In reaching this conclusion, the court began its analysis at the time the documents were compiled. The court stressed the confidential treatment of the documents at the time of and subsequent to their composition, noting that in *Upjohn* the Court had stressed that the documents were "considered ‘highly confidential’ when made . . . and have been kept confidential by the company." The *Raytheon* court then looked at the number of company personnel with authorized access, noting that "[t]he presence of nonessential third parties not needed for the transmittal of the information will negate the privilege."

The *Raytheon* court found that the distribution of the documents was both "reasonable and necessary" in that all those who received copies had a status that indicated that it was "essential that they know the contents of the memorandum." The court then pro-

101. *Id.*  
102. 93 F.R.D. 138 (D. Del. 1982).  
103. *Id.* at 142.  
106. 93 F.R.D. at 141 (citing *Pitney-Bowes, Inc. v. Mestre*, 86 F.R.D. 444, 446 (S.D. Fla. 1980)).  
107. 93 F.R.D. at 141 (citation omitted).
ceeded to the question of whether the documents, marked "company private" and filed in the general corporate project file, lost their confidential status because the file was open to employees working on the particular project file.\(^{108}\) The party arguing that the documents had been published and the corporate attorney-client privilege thus waived cited the recent case of \textit{Coastal States Gas Corp. v. Department of Energy}.\(^{109}\) In \textit{Coastal}, the Department of Energy ("DOE") had opposed the disclosure of certain documents under exemption 5 of the Freedom of Information Act, arguing that the documents were protected by the attorney-client privilege.\(^{110}\) The \textit{Coastal} court held that DOE had waived the privilege because it could not demonstrate that it had treated the documents in a confidential manner.\(^{111}\) The \textit{Raytheon} court concluded, however, that \textit{Coastal} was distinguishable because the documents in \textit{Raytheon}, unlike those in \textit{Coastal}, "were not broadly circulated or used as training materials; they were simply indexed and placed in the appropriate file where they would be available to those corporate employees who needed them."\(^{112}\) As the court had pointed out in \textit{Coastal}, it is only when facts have been made known to persons other than those who need to know them that confidentiality is destroyed.\(^{113}\) The \textit{Raytheon} court also distinguished \textit{Coastal} by noting that the \textit{Coastal} court had written its decision prior to \textit{Upjohn}, which rejected the "control group test" that \textit{Coastal} had used.\(^{114}\) The \textit{Raytheon} court concluded as follows:

\begin{quote}
[T]he fact that some unauthorized corporate personnel may purposely or inadvertently read a privileged document does not render that document nonconfidential. To hold otherwise would be to require every corporation to maintain at least two sets of files. Moreover, a screening committee would then have to be set up whereby some designated official could pass on the need of each employee to know the contents of any requested document. Such a system is neither practical nor in the Court's opinion required by the case law.\(^{115}\)
\end{quote}

\(^{108}\) \textit{Id.} at 142.
\(^{109}\) 617 F.2d 854 (D.C. Cir. 1980).
\(^{110}\) \textit{Id.} at 862.
\(^{111}\) \textit{Id.} at 863-64.
\(^{112}\) 93 F.R.D. at 142.
\(^{113}\) 617 F.2d at 863.
\(^{114}\) 93 F.R.D. at 142.
\(^{115}\) \textit{Id.} (emphasis added).
The reasoning of the court in Raytheon may be applicable to files kept in a computer maintained or controlled by outside service organizations only where these organizations are considered agents, either implied or because of express confidentiality obligations made by the organization, which would give them the status of agents for these limited purposes. Such an arrangement would show the client's intent to maintain confidentiality. The use of outside organizations for the maintenance or storage of computer data bases places the need to maintain confidentiality one step further removed from the situation in Raytheon, as personnel other than the corporation's employees will have access to the confidential information. Consequently, the most important aspect of Raytheon may be the fact that it raised, rather than truly answered, the question of what happens when confidential documents are filed with general corporate documents.

Absent the adoption of one or more of the above theories to sustain the attorney-client privilege, counsel may wish to carefully consider the ramifications of using data processing for storage and transmission of client communications. As we suggest later in this article, however, there are several steps that can be taken by both the attorney and the client to assist in maintaining the privilege.

B. Work Product Doctrine

The work product doctrine, enunciated in Hickman v. Taylor,\(^{118}\) provides a qualified privilege against disclosure for materials prepared by the attorney in anticipation of litigation. Although related to the attorney-client privilege, it differs in that the attorney is the holder of the privilege and it is a "qualified" privilege. Despite the highly sensitive or confidential nature of the information contained in the documents, they are discoverable if the moving party can show "substantial need" or "undue hardship."\(^{117}\) In some instances, the

117. Rule 26 of the Federal Rules of Civil Procedure provides, in part:
Subject to the provisions of subdivision (b)(4) of this rule, a party may obtain discovery of documents and tangible things otherwise discoverable under subdivision (b)(1) of this rule and prepared in anticipation of litigation or for trial by or for another party or by or for that other party's representative (including his attorney, consultant, surety, indemnitor, insurer, or agent) only upon a showing that the party seeking discovery has substantial need of the materials in the preparation of his case and that he is unable without undue hardship to obtain the substantial equivalent of the materials by other means. In ordering discovery of such materials when the required showing has been made, the court shall protect against disclosure of the mental impressions, conclusions, opinions, or legal theories of an attorney or other
work product doctrine can afford broader protection than the attorney-client privilege because disclosure to others may not constitute waiver. Disclosure to those who are not "clients," for example, does not constitute waiver. The doctrine was intended to create a "zone of privacy" within which the attorney may think, plan, weigh facts and legal theories, and prepare the case.\textsuperscript{118} This policy can be satisfied by less than complete secrecy; therefore, disclosure of work product documents will not constitute waiver unless the disclosure is inconsistent with maintaining the secrecy from the possible or actual adversary.\textsuperscript{119}

To be protected, the document or materials must have been prepared "in anticipation of litigation," which can be somewhat difficult to show. Generally, opinion or mental impression work product prepared by counsel will be immune from discovery,\textsuperscript{120} at least in part because of its inherent lack of reliability as evidence. In contrast, materials or documents prepared for counsel involve less of an intrusion into an attorney's privacy and thus are more susceptible to discovery. Some courts will strictly enforce the work product doctrine with a few limited exceptions.\textsuperscript{121} Other courts balance the amount of opinion work contained in the requested material against the requesting party's need for the information.\textsuperscript{122}

The Federal Rules of Civil Procedure protect work product materials from discovery unless the discovering party shows: (1) substantial need and (2) inability "without undue hardship to obtain the substantial equivalent" by other means.\textsuperscript{123} Once this showing is made, "ordinary" work product can be discovered; yet "opinion" work product, "the mental impressions, conclusions, opinions, or legal theories of an attorney" or other party concerning litigation may still be protectable.\textsuperscript{124} With increased use of data processing equip-
ment for document creation, the potential for having work product information stored on computer data banks is perhaps even greater than it is for the storage of attorney-client privilege material. However, there is no plausible reason why the work product doctrine should not be applicable to information stored in a computer.

One possible way to protect work product from discovery is to insert a code or comment involving opinion or strategy, to elevate the work from ordinary work product to opinion work product and thereby increase its chances of not being discovered. That approach can be challenged, however, and may not be upheld. The better approach, which appears well suited for information stored in a computer, is to meet the issue directly and argue that legal theories are inherently and inextricably woven into the data.126

It may be necessary, even under that approach, to let the court review the data in camera, and the non-opinion portions may then be discoverable. In fact, due to the ability of a computer to excise critical portions, a court may be more willing to tolerate fishing expeditions into work product stored in a computer.

At least one court has suggested that a document containing an attorney’s mental impressions that cannot be separated from the factual content is obtainable, so long as the requesting party meets the requirements of Rule 26(b)(3) of the Federal Rules of Civil Procedure.126 This reasoning could be countered by the Hickman admonition that only a “rare situation” can justify intruding into the attorney’s mental impressions.127 Counsel should insist on an in camera review of the documents to glean the factual material that would then be furnished to the discovering party.128

Federal civil procedure rules permit the discovery of computer records in readable form (printouts), just as manual records are discoverable.129 But in IBM Peripherals EDP Devices Antitrust Litigation,130 where the plaintiffs wished to compel the use of the defendant’s document retrieval system in answering interrogatories as to the identity of certain documents, the court ruled that there had

125. See generally Harper & Row Publishers, Inc. v. Decker, 423 F.2d 487 (7th Cir. 1970); In re Murphy, 560 F.2d 326 (8th Cir. 1977).
been no showing of substantial need, that the material had been placed in the data base in anticipation of litigation, and that such information was still available by other means.\textsuperscript{131} The judge also noted the defendant’s argument that the discovering party would also learn which key documents and words the defendant considered significant, thus permitting the party to learn some of the defendant attorney’s mental impressions.\textsuperscript{132}

Work product materials will not be rendered discoverable in all cases simply because the material has been placed in a data base, and no party should be compelled to give the discovering party total access to its system. Rather, discovery must be limited to specific documents and specific information, and the discovering party must make the required showing of substantial need.

\subsection*{C. Other Testimonial Privileges.}

1. \textit{Accountant-Client}.—The accountant-client privilege is entirely a creation of state statute. The common law rule is that no privilege attaches to the transactions between an accountant and client absent a statute creating a privilege.\textsuperscript{133} Federal law does not recognize an accountant’s privilege,\textsuperscript{134} nor will a state-created privilege be recognized in a federal criminal trial.\textsuperscript{135}

Where an attorney is acting as an accountant, courts have not only failed to find an accountant’s privilege, but have held that any client-accountant transaction does not bring the communications

\begin{itemize}
\item\textsuperscript{131} \textit{Id.}
\item\textsuperscript{132} \textit{Id.} A computer litigation support system may be subject to discovery since this system is merely a tool used by the attorney to code documents based on objective indexing methods and is, therefore, discoverable as ordinary work product just as any other manual file system would be. Because a party may discover “the existence, description, nature, custody, condition and location of any books, documents or tangible,” Fed. R. Civ. P. 26(b)(1), the owner of a computer support system should be able to claim no more privilege than the owner of a manual file system because the owner of the computer-stored information can also reduce the computer-stored information to “hardcopy” form. Further, there are no subjective thought processes in this type of index system that would arguably make this information “opinion” work product. Unless the documents are indexed by a method that might reveal the attorney’s thought processes or strategy — perhaps indexing by legal issues — this material could be discoverable.
\item\textsuperscript{133} Himmelfarb v. United States, 175 F.2d 924, 931 (9th Cir. 1949). For an example of a statutorily created accountant-client privilege, see COLO. REV. STAT. § 13-90-107(f) (1973); IND. CODE ANN. § 25-2-1-23 (West 1980); NEv. REV. STAT. § 49.185 (1979).
\item\textsuperscript{134} Couch v. United States, 409 U.S. 322, 335 (1973); United States v. Wainwright, 413 F.2d 796, 803 (10th Cir. 1969); Falsone v. United States, 205 F.2d 734, 739 (5th Cir.), cert. denied, 346 U.S. 864 (1953).
\item\textsuperscript{135} United States v. Culver, 224 F. Supp. 419, 434 (D. Md. 1963).
\end{itemize}
within the attorney-client privilege. An accountant who has been hired by an attorney may or may not be able to invoke the attorney-client privilege on the theory that the accountant was the attorney's agent. In United States v. Kovel, the court held that the attorney-client privilege was applicable to an accountant in the attorney's employ if the communication was made for the purpose of obtaining legal advice. In Himmelfarb v. United States, the court stated that where the presence of a third person is indispensable to the communications between attorney and client, the privilege may be invoked. The Himmelfarb court held that in that case the accountant's presence was not indispensable, but was merely a convenience that effectively waived the confidentiality of the privilege.

Those statutes that recognize the accountant-client privilege do so on the same basis as the attorney-client privilege. The accountant-client communication must be made in the course of professional employment and may generally include under its umbrella the accountant's stenographer, clerk, secretary or assistant. The Nevada statute defines a confidential communication as one that is "not intended to be disclosed to third persons other than those to whom disclosure is in furtherance of the rendition of professional account-

137. 296 F.2d 918 (2d Cir. 1961).
138. Id. at 921-22.
139. 175 F.2d 924 (9th Cir. 1949).
140. Id. at 939.
141. Id. This reasoning is critically important to the issue of whether disclosure of confidential communications to a data processing employee or outside service organization employee constitutes waiver. By this court's reasoning, if the computer technician's presence is "merely a convenience" rather than indispensable to facilitating attorney-client communications, the privilege will be deemed waived. The answer that any particular court may give to this question may be based on policy considerations revolving around testimonial privileges, as well as the court's view of technological innovation and its integration into the legal system.
143. Colorado law provides:
A certified public accountant shall not be examined without the consent of his client as to any communication made by the client to him in person or through the media of books of account and financial records, or his advice, reports, or working papers given or made thereon in the course of professional employment; nor shall a secretary, stenographer, clerk, or assistant of a certified public accountant be examined without the consent of the client concerning any fact, the knowledge of which he has acquired in such capacity.
Because of the nature of the work, it is likely that an accountant’s work product will be stored in a computer. Consequently, the accountant will probably encounter the same problems with the accountant-client privilege as an attorney will with the attorney-client privilege. Given the similarity of the two privileges, the accountant should be able to make the same arguments as the attorney in maintaining the confidentiality of computer files, and courts should treat the two privileges similarly with regard to what will constitute a waiver of the confidentiality of the computer-stored data.

2. Other Privileges.—Evidentiary privileges have also been extended to other relationships for substantially the same purpose as that for which the attorney-client privilege exists. The origin of most privileges is in the common law, but many states have enacted statutes that either codify these common law privileges or add more unusual types of privileges to those already recognized by the common law. State statutes protect confidential communications between psychologists or psychiatrists and patients; physicians or surgeons and patients; clergy and penitents; and accountants and clients. Other more unusual protections include: parent or legal guardian and child; pathologist or audiologist and patient; reporter and informant; juvenile or probation officer and client; and teacher or school counselor and pupil. These privileges generally require that the communication be made privately and that it

CONFIDENTIALITY AND COMPUTERS

not be intended for further disclosure except to other persons in furtherance of the purpose of the communication. It would thus appear that the same arguments and problems exist with respect to these privileges as exist for the attorney-client privilege.

If maintaining confidential communications in computers automatically results in a waiver of the confidential and privileged status of the communications due to the presence of third party data processing personnel, the shock waves will reach far beyond the law office. This will be especially true as more institutions — legal, governmental, educational, and medical — utilize the efficiency of the computer. In the face of widespread computer usage, it is inconceivable that public policy could best be served by destroying the very basis on which these special relationships exist.


The principle of confidentiality is relevant not only in regard to testimonial privileges, but also in regard to the Model Code of Professional Responsibility. Ethical Consideration 4-3 states that:

Unless the client otherwise directs, it is not improper for a lawyer to give limited information from his files to an outside agency necessary for statistical, bookkeeping, accounting, data processing, banking, printing, or other legitimate purposes, provided he exercises due care in the selection of the agency and warns the agency that the information must be kept confidential.

This Ethical Consideration is clearly applicable to the situation wherein an outside service organization is employed by a corporation.

155. The American Bar Association adopted the Model Code of Professional Responsibility in 1969 and it became effective on January 1, 1970. MODEL CODE OF PROFESSIONAL RESPONSIBILITY Preface (1980). The Code was “designed to be adopted by appropriate agencies both as an inspirational guide to members of the profession and as a basis for disciplinary action when the conduct of a lawyer falls below the required minimum standards stated in the Disciplinary Rules.” Id. at Preliminary Statement.

Although the Model Code of Professional Responsibility has been replaced by the Model Rules of Professional Conduct, the new Model Rules have not yet been widely adopted. New York Times, Aug. 3, 1983, at A1, col. 1. The Code of Professional Responsibility admonishes a lawyer “to preserve the confidences and secrets of a client.” MODEL CODE OF PROFESSIONAL RESPONSIBILITY Canon 4 (1980). Disciplinary Rule 4-101(A) makes clear that the Canon encompasses more than privileged information:

“Confidence” refers to information protected by the attorney-client privilege under applicable law, and “secret” refers to other information gained in the professional relationship that the client has requested be held inviolate or the disclosure of which would be embarrassing or would be likely to be detrimental to the client.

MODEL CODE OF PROFESSIONAL RESPONSIBILITY DR 4-101(A).

156. MODEL CODE OF PROFESSIONAL RESPONSIBILITY EC 4-3 (1980).
or law firm to maintain its computer equipment. Although the Ethical Considerations are not mandatory, and merely represent objectives toward which members of the profession should strive,\footnote{157} the Disciplinary Rules ("DR")\footnote{158} provide: "A lawyer shall exercise reasonable care to prevent his employees, associates and others whose services are utilized by him from disclosing or using confidences or secrets of a client, except that a lawyer may reveal the information allowed by DR 4-101(C) through an employee." Rule 4-101(D)\footnote{159} seems to indicate that the attorney's duty would not be violated by engaging the services of an outside organization's computer technicians even though this might involve allowing access to a client's confidential information, as long as the attorney used reasonable care to prevent disclosure. It would also seem that the maintenance of computers is less likely to involve access to confidential files than the situations envisioned by the Rules and Ethical Consideration. Outside data processing firms, however, would be intimately involved in manipulating client information provided by the law firm, rather than merely servicing software or hardware that might involve the computer technician's use of a confidential file.

The American Bar Association's Standing Committee on Ethics and Professional Responsibility,\footnote{160} in issuing an informal opinion,\footnote{161} questioned whether a law firm had a duty to inform the client that it was using a data processing firm.\footnote{162} The committee assumed that the information that would be provided to the service bureau would include client identification information involving client numbers, client names, detailed descriptive information, involving work performed by the attorney on specified dates, concerning particular matters for identified clients, financial information, and documents

\footnote{157} MODEL CODE OF PROFESSIONAL RESPONSIBILITY Preliminary Statement (1980).

\footnote{158} Disciplinary Rules, unlike Ethical Considerations, are mandatory in character and set forth minimum levels of conduct which all lawyers must reach or face disciplinary action. Id.

\footnote{159} MODEL CODE OF PROFESSIONAL RESPONSIBILITY DR 4-101(D) (1980).

\footnote{160} The American Bar Association's Standing Committee on Ethics and Professional Responsibility, composed of eight practitioners who are elected by majority vote of the American Bar Association's members, is charged with the duty of interpreting the Model Code of Professional Responsibility. 1 ABA COMM. ON ETHICS AND PROFESSIONAL RESPONSIBILITY, INFORMAL ETHICS OPINIONS 5 (1975).

\footnote{161} Informal Opinions are issued by the Committee in response to specific inquiries from individual members of the ABA. The Committee also issues Formal Opinions, which are issued to deal with matters of general interest in the profession. Id.

being prepared by computerized word processing. 163 The committee stated that "the use of outside agencies for statistical, bookkeeping, accounting, data processing, banking, printing, and other legitimate purposes is comparable to the use of employees and associates and, accordingly, is embraced within" Disciplinary Rule 4-101(D).

In reviewing plans to set up a private agency that would provide off-site word processing and retrieval for attorneys, the committee stressed that its philosophy was to interpret ethical standards so as to permit the use of modern business practices, stating that:

[It] really makes no difference as to whether or not the contemplated data processing was done in the law office by an employee or in the place of business of the data processor. The key is that whoever it is that is handling the material, whether or not he is a formal employee of the law firm or an employee of a contractual agent of the law firm, must preserve the confidences of the client . . . 164

The committee thus concluded that there would be no ethical code violation in not informing a client that a data processing firm was being used so long as the arrangements were made in such a manner "that the material be kept in confidence and the employees of the law firm and the data processor do so keep them in confidence and do not permit disclosure to any unauthorized person." 165 The committee formulated a four part test to determine whether the attorney had taken due care in choosing the agency to which limited information was to be given: "1. the appropriate selection of the agency; 2. the appropriate rules within the agency for the preservation of secrecy; 3. the appropriate warning to the agency; 4. the ability of the agency to keep its matters secret." 166

Although these opinions are not binding on code enforcers 167 and reflect professional and ethical concerns rather than legal standards for the maintenance of evidentiary privileges, the opinions offer enlightenment as to what might be considered reasonable con-

163. Id.
165. Id. at 337.
166. Id.
167. Lawyers are disciplined by appropriate state and local bar associations, acting through the local courts or under the rules of those courts. Since each state has enacted its own rules of professional conduct that regulate its lawyers, the Model Code of Professional Responsibility, and the opinions issued interpreting the Code, will not be directly enforceable in any state. American Bar Association, Professional Responsibility, A Guide for Attorneys 15-17 (1978).
duct on the part of an attorney to maintain privileges in the face of new methods and systems of information storage. Thus, the reasonable conduct or due care of the Model Code of Professional Responsibility might be used in part to flesh out the meaning of "reasonable precautions" when the term is used by courts, such as in In re Grand Jury Proceedings Involving Berkley and Co., Inc., in determining the privileged status of attorney-client information.

The key to the lawyer's responsibility in handling confidential client information would appear to be found in EC 4-3's requirements of due care in the selection of an agency and the notice or warning to the agency that the information must remain confidential. These considerations point toward the use of confidentiality or non-disclosure agreements signed by the agency. Due care may also involve an inquiry into the agency's rules for maintaining secrecy. Consequently, in making a decision as to whether to place confidential client information on computer data bases, the attorney may have a duty to inform the client of the possibility of the waiver of a privilege because of the disclosure to an outside agency and permit the client to decide whether to assume the risk of waiver or disclosure. This procedure would be in keeping with the theory that the privilege belongs to the client, who ultimately possesses the right to either claim the privilege or waive it.

III. CONFIDENTIAL BUSINESS INFORMATION

The nature of certain confidential business information is such that it remains valuable only so long as the information remains secret. Once confidential business information is disclosed, its value to

168. Id.
170. The new Model Rules of Professional Conduct take essentially the same approach as did the Model Code of Professional Responsibility with respect to the disclosure of confidential information to employees. Rule 5.3 states:

With respect to a nonlawyer employed or retained by or associated with a lawyer: (a) A partner in a law firm shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the person's conduct is compatible with the professional obligations of the lawyer . . .

MODEL RULES OF PROFESSIONAL CONDUCT Rule 5.3.

The comment to this rule states: "[a] lawyer should give [employees] appropriate instruction and supervision . . . particularly regarding the obligation not to disclose information relating to representation of the client . . ." Id. Thus, the Model Rules, as does the Model Code, appear to allow disclosure of confidential client information to employees as long as the attorney takes reasonable precautions to prevent disclosure. However, it would appear that as a minimum, the Model Rules require some sort of instructions to employees regarding their duty not to disclose confidential information before the "reasonable efforts" standard can be met.
the holder of the information is lost: the holder no longer will have the competitive advantage that the information provided. Maintaining the confidentiality of certain business information is as important to its holder as maintaining confidences is to the holder of one of the other testimonial privileges. The difference, however, is one of protecting information as opposed to protecting communications.\textsuperscript{171}

Business information protected by a patent or copyright may be disclosed without risk of losing the value of the information. Patents and copyrights are protected only for a statutory period,\textsuperscript{172} however, and it may be desirable to achieve longer protection. If a company wishes to use the information for its own competitive advantage rather than disseminate the information, it can be protected only by keeping the information as a trade secret.\textsuperscript{173}

The term “trade secret” is defined by the Restatement of Torts “Restatement” as

any formula, pattern, device or compilation of information 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. . . . It differs from other secret information in a business in that it is not simply information as to single or ephemeral events in the conduct of the business, as for example, the amount or other terms of a secret bid for a contract or the salary of certain employees. . . . A trade secret is a process or device for continuous use in the operation of the business. . . .\textsuperscript{174}

The term trade secret has been further defined as information that is secret, novel and has value.\textsuperscript{175}

The following discussion examines whether disclosure of a trade secret to data processing personnel constitutes an abandonment of secrecy, thus causing the information to lose its status as a trade

\begin{itemize}
  \item \textsuperscript{171} When confidential business information is made available to an attorney for the purposes of representation, it should not lose status as a trade secret, nor its status as being within the attorney-client privilege. Presuming that the law firm or the corporate law department is enforcing strict controls over computer access in order to maintain the higher standards of attorney-client nondisclosure, the trade information existing in the data banks should not lose its trade secret status.
  \item \textsuperscript{172} The constitutional basis for federal patent protection is found in U.S. CONST. art. I, § 8. See, 35 U.S.C. §§ 1-376 (1977), for patent statutes and 17 U.S.C. §§ 101-810 for copyright statutes.
  \item \textsuperscript{173} \textit{Restatement of Torts} § 757 comment b, at 5 (1939).
  \item \textsuperscript{174} \textit{Id.}
  \item \textsuperscript{175} 9A Z. CAUITCH, BUSINESS ORGANIZATIONS WITH TAX PLANNING § 232.01[2] (1982).
\end{itemize}
secret. Although secrecy is a fundamental element of a trade secret, absolute secrecy is not required to maintain the privilege of non-disclosure. Courts have recognized that only a "substantial element" of secrecy is required. A limited disclosure for a restricted purpose does not, therefore, ordinarily result in an abandonment of the element of secrecy. Moreover, courts have held that the existence of confidential circumstances surrounding the disclosure of a trade secret tends to negate the abandonment of secrecy.

The Restatement states that it is not required that only the proprietor of the business have knowledge of the secret. The proprietor may disclose the trade secret to those who have been pledged to secrecy. A substantial element of secrecy must exist, however, so that the information would be difficult to be legitimately acquired. Two of the factors suggested by the Restatement for determining whether a trade secret exists are "the extent of measures taken by [the holder] to guard the secrecy of the information," and "the extent to which the information is known by employees and others involved in his business."

The importance of the confidential circumstances surrounding the limited disclosure of a trade secret was recognized in United States Plywood Corp. v. General Plywood Corp. In that case, the court stated that there was no evidence of any effort on the part of a plywood finish developer to maintain secrecy because the developer did not require the licensees of the process to sign confidentiality agreements. Furthermore, in J.T. Healy & Son, Inc. v. James A. Murphy & Son, Inc., where a manufacturer chose not to warn his employees against disclosing trade secrets because of fear that treating the secret processes in a special way would excite undue interest in those processes, the court rejected his argument and held that this ploy was totally contrary to the general rule that businessmen

176. See id. at § 232-33 and cases cited therein.
178. See, e.g., id.
179. RESTATEMENT OF TORTS § 757 comment b (1939).
180. Id.
181. Id. See Clark v. Bunker, 453 F.2d 1006, 1009 (9th Cir. 1972).
182. RESTATEMENT OF TORTS § 757 comment b (1939).
184. Plywood, 370 F.2d at 508.
186. 357 Mass. at 737, 260 N.E.2d at 730.
must be eternally vigilant to guard the secrecy of a trade secret—preferably by warnings to employees, and the signing of confidentiality employment agreements.\textsuperscript{187}

Under the Plywood analysis, it appears that a trade secret would not be abandoned by a business if the employees who have access to computer data banks are operating under written obligations of confidentiality. This would be equally true of a law firm’s employees, where the firm’s corporate client was required to turn over certain trade secret information to the law firm. The law firm would already be in a confidential attorney-client relationship with the corporation, and the confidential obligations would exist in the absence of a written agreement and would extend to the law firm’s employees under an agency theory.

Use of third party service organizations, however, may cause the protection to be lost. Abandonment of secrecy has been established in certain cases where methods of operation and equipment were visible because of access to manufacturing facilities through tours. In Shatterproof Glass Corp. v. Guardian Glass,\textsuperscript{188} for example, the court noted that the glass manufacturer’s customers, dealers, distributors and others could view the glass bending operations, and, although there was evidence of security and nonsecurity routes for the tours, neither route was defined and those who took the tour were not pledged to secrecy.\textsuperscript{189} In Loundes Products, Inc. v. Brower,\textsuperscript{190} the court held that the manufacturer’s trade secret was not entitled to protection because of lax security and open access throughout the plant by all employees.\textsuperscript{191} Such cases indicate that the signing of confidentiality agreements by employees, standing alone, may be insufficient to show an intent to maintain confidentiality. It is analogous to a third party service organization having full access to computer files containing trade secret information. Such access could be compared with the tours in Shatterproof Glass, and thus result in a waiver of secrecy.

Therefore, to avoid such ambiguity, it is necessary to develop clearly delineated procedures for computer access on a “need to know” basis. These arrangements could include restricting access to employees and outside service organizations except where computer

\begin{thebibliography}{9}
\bibitem{187} 357 Mass. at 738, 260 N.E.2d at 730-31.
\bibitem{189} \emph{id.} at 864.
\bibitem{190} 259 S.C. 322, 191 S.E.2d 761 (1972).
\bibitem{191} 259 S.C. at 329-30, 191 S.E.2d at 765-66.
\end{thebibliography}
maintenance circumstances require that a confidential data bank be used to correct the computer problem, and requiring secrecy agreements of all persons, in-house and outside, who have access to the computer. Indeed, the authors recommend that a manual of computer security be developed, incorporating the security procedures, in order to demonstrate an intent to maintain the secrecy of the information.

IV. Recommendations And Solutions

Of the various types of confidential information that have been discussed, it would appear that the most rigorous standard for non-disclosure applies to the maintenance of the attorney-client privilege. Consequently, if the security measures taken to guard computer data bases are sufficiently strict to preserve the attorney-client privilege, it should follow that those procedures would be adequate for other privileges and trade secrets as well. The following are recommendations for maintaining the confidentiality of computer stored information that should provide sufficient protection to establish “reasonable precautions” for preservation of the attorney-client privilege. Greater measures may be required in a particular situation, and the lawyer or business person should take such additional steps as are necessary for that situation. It is also suggested that the following recommendations be incorporated into a mandatory computer security manual for the law firm or corporation, and be adopted as firm or corporate policy.

A. Computer Security Procedures

As suggested by Slivka and Darrow, the security of a data system will generally depend on systems controls, physical access controls and administrative controls.\textsuperscript{192} Systems controls consist of identification, authorization, and privacy transformations.\textsuperscript{193} The first step in implementing systems controls is to limit access to a computer system by requiring the identification of the computer user. This can be accomplished by allowing access only through use of a password or log-on procedure. More complicated systems might include a code designating a department or firm in addition to the individual password.

\textsuperscript{192} Slivka & Darrow, \textit{Methods and Problems in Computer Security}, 5 J. Computers \& L. 217, 228 (1976). A detailed analysis of security procedures is found in this excellent article. The categories of security procedures are suggested by this work.

\textsuperscript{193} \textit{Id.} at 229-46.
Access can be further limited by an authorization that signifies the functions that a user is authorized to perform within the system. For example, a user could be allowed to perform all, only some or none of several functions on a file. A user might be allowed to check the information in a file, but not be allowed to alter or add to the file. Consequently, without authorization, certain information would not be available to all users of a system. The more complicated and extensive the information stored in the system, the more horizontal levels of access can be created, with the system's users capable of attaining access only to their authorized levels. Information can also be departmentalized in a vertical division among users and departments, so that one department cannot use another department's files unless authorized to do so by that department. Further, the level of authorization can be extended to control access to specific records or even parts of records. A payroll clerk, for example, may be authorized to gain access to payroll information in a personnel file but may not be able to gain access to performance ratings located in the same personnel file.¹⁹⁴

A more sophisticated system control is to use privacy transformations to protect confidential information. Privacy transformations render data unintelligible to unauthorized inquiries and, thus, involve a more serious and concomitantly more complicated attempt at maintaining secrecy. Although this method is probably too expensive and troublesome for a law firm to institute, it could be used more realistically by a large corporation with a computer system that has the capability of storing large amounts of corporate information.

1. Physical Controls.—Physical controls to access to confidential data are linked to system controls. Unauthorized use can be physically controlled by requiring sign-in logs, the use of key lock or card access systems, or by placing the terminal that has sole access to a confidential computer file in a secured room, just as confidential manual files are often placed in a single room with limited access. This may be difficult if a legal department or firm has placed computer terminals in all offices. In this instance, the password and code system would have to be implemented to limit access.

With larger systems, time and location of access can be recorded for consulting at a later date. This may be particularly useful when access is permitted by telephone modems from off-site locations, either by persons using the system or by maintenance vendors.

¹⁹⁴. Id. at 237.
2. Administrative Controls.—Administrative controls assure that personnel are informed of the proper steps to take in implementing a secure system. In a corporate setting, it is necessary for the legal, accounting, and data processing departments to cooperate to establish a secure system. For purposes of the attorney-client privilege, the managers of a data processing department should be informed that they and their employees are agents of the legal department for the purpose of maintaining the confidentiality of the legal department's information contained in the computer data base. This can be accomplished by a formal memorandum outlining the steps to be taken to protect information prepared by the legal department and submitted to the data processing department for storage in the computer system. This memorandum, together with any later directives dealing with confidential files, should become part of the computer security procedures manual.

The memorandum to the head of the data processing department should outline, as a minimum, the following duties of the data processing manager:

1. Inform employees of the obligation of confidentiality and their status as agents of the legal department.
2. Inform vendors and maintenance personnel servicing equipment or software programs containing legal department information that the information is confidential, and to take such steps as necessary to evidence knowledge of such actions as the legal department may direct, including the signing of consent forms.
3. Prohibit access to equipment containing legal department information to all unauthorized personnel.
4. Inform the head of the legal department of any unauthorized access, the time and date thereof, and the information affected.
5. Document, as directed by the legal department, the services performed and maintenance rendered on equipment and programs containing legal department information.
6. Take all reasonable steps to protect the contents of tapes and other back-up material containing legal department material that may be delivered to third parties for off-site storage.
7. Require new data processing personnel to be adequately advised of their obligation of confidentiality with respect to legal department information.
8. Assist the legal department in establishing special files that restrict access to authorized law department personnel.

With some modifications, this type of memorandum could also be used for internal control by a law firm, and for purposes of in-
forming timesharing services of their responsibilities.

B. Legal Staff Procedures

In addition to computer security procedures, it is also important that internal procedures be established when attorney-client information is to be stored in computer data bases. The following procedures are suggested:

1. Develop levels of accessibility, both horizontally, for certain types of information, and vertically, as between departments, and identify the members of each level. In a corporate setting, this might be done by job title, according to organizational charts. In a smaller setting, within a corporate legal department, there may be no need to have differing levels of accessibility, with all attorneys having equal access to confidential files. Criteria should be adopted to identify how information/communications will receive “confidential” designation.

2. Documents that constitute communications to the attorney, work product or trade secrets should be designated and their legal status clearly reflected on the document.

3. Access to these documents should be strictly controlled by maintaining a distinct set of files for confidential documents. This would obviously require the attorney to designate which documents are confidential, thus requiring special input into the separate data bank. The log of entries into the data bank should also reflect the confidential nature of the document.

4. Access to the confidential data base by data processing personnel and outside service organizations, and the reasons for such access, should be recorded by log book. Any unauthorized entries should be immediately reported to the corporate legal department or law firm.

5. “Need to know” access may be restricted to those employees who are members of the decision-making group, the attorney’s subordinates, and experts retained for the purpose of assisting in legal advice. If personnel have only limited access to such confidential data banks (i.e., access only where the specific computer difficulty involves the confidential data base, or the creation of back-up files, or if access to such files is permitted only upon authorization from higher level personnel or the law department), this limited and carefully supervised access should be sufficient to sustain at least the intent of the client to maintain the confidentiality of files. It should be noted that, in many instances, these employees sign confidentiality obligations as part of their employment contracts. Further, the access to confidential computer files by such personnel could be limited to those situations in which the system has “crashed” during the use of the confidential file and the technician must, therefore, correct the problem while using the sensitive file.

6. Although in James Julian, Inc. v. Raytheon Co., 93 F.R.D. 138 (D. Del. 1982), see supra notes 102-15 and accompanying text, a separate confidential file was not required, this recommendation urges extra caution.
5. Any hard copy of computer-stored information should, if possible, be stored separately from non-confidential files and access should be strictly limited on the same basis as that for computer files.
6. The authorization for data processing personnel or outside service organizations to work on confidential files should come directly from the concerned attorney to preserve confidentiality on an agency theory.

C. Employment Agreements

Employment agreements are a method of placing nondisclosure understandings in contract form. These confidentiality agreements could be especially important in the maintenance of trade secrets because the use of such contracts would indicate the holder's intent to maintain secrecy. Furthermore, confidentiality agreements signed by data processing personnel could also be used to indicate a similar intent to the court. Since employees who have knowledge of trade secret information pose a potential threat to the preservation of secrecy if they should leave the firm, confidentiality provisions should be made a part of employment contracts, often with accompanying covenants not to compete against the employer.¹⁹⁷ These employee agreements should state:

1. That the employee may have access to company confidential proprietary information or trade secrets;
2. That in regard to this information, the company may be under obligations of confidentiality to others;
3. That such information should be kept confidential by the employee and should not be disclosed to any third party, directly or indirectly, without the prior written consent of the company;
4. That, upon termination of employment, any information or data developed during employment which is the property of the company should be returned to the company.

D. Confidentiality Obligations of Outside Service Organizations

Outside service organizations may be resistant to signing nondisclosure agreements, since they will not voluntarily choose to acquire additional potential liabilities. However, because the agency theory is more tenuously applicable to these outside organizations,

non-disclosure agreements from these groups are very important and should include at least the following provisions:

1. The vendor should acknowledge that under the terms of the service agreement, the service organization may have access to hardware or software with respect to which the law firm or corporation may be under obligations of confidentiality to others, or which may contain confidential/proprietary information or trade secrets of the law firm or corporation or other parties.

2. The service organization should agree to maintain and cause its employees, servants and agents to maintain the confidentiality of all trade secrets, business or financial information, software programs and content, and any and all information, data, reports, analysis whatsoever, disclosed or otherwise made available to, or obtained by the service organization’s performance of, services under the agreement.

3. The service organization should agree to supply the names of its employees, servants or agents who will have access to such confidential/proprietary information or the service organization should require each of these persons to provide the law firm or corporation a written acknowledgement that the confidentiality obligations under the agreement have been read and understood by these employees, and should further agree to provide updates as personnel change.

4. There should be a reasonable limit on the length of time the confidentiality agreements are enforceable after the termination of the service or employment agreement, within which the confidentiality obligations are maintained.

It should be recognized that the vendor’s fear of accepting liability under these circumstances may make an agreement on non-disclosure provisions difficult to reach, and success may well depend on the bargaining strength of the customer. One possible approach that may alleviate the vendor’s concerns would be to simply agree that, with regard to privileged matters, damages are waived and the parties consent only to injunctive relief. Of course, that approach

198. The Foreign Corrupt Practices Act, 15 U.S.C. § 78dd-2 (1982), makes certain payments by issuers of securities to foreign officials or other foreign persons illegal, and therefore requires such issuers to maintain accurate records. The law requires the issuer to “devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that . . . access to assets is permitted only in accordance with management’s general or specific authorization . . . .” Id. at § 78m(b)(2)(B)(i) (emphasis added). This duty to take reasonable precautions to protect the assets of the corporation implies a duty to require confidential agreements.
would probably not be useful for trade secrets.  

These written obligations act as notice or warning to the service organization that it may have access to certain proprietary information that the law firm or corporation expects the service organization to treat with care. If such contractual agreements cannot be obtained, it is suggested that notice be given to the organization in some other form, such as a letter of understanding, that informs the service person at the commencement of the service that information contained in the computer should be kept confidential.

V. Conclusion

The changing methods of storing information brought about by the developing computer and communications technology compel a new look at the treatment of confidential information in both the legal and business setting. At present, there is little case law indicating how courts will view these technological changes and whether they will permit the creation of data bases containing confidential or privileged business information to be free from discovery. Although absolute secrecy is not necessary to sustain trade secret protection, strict protection should still be accorded trade secrets contained on computer data bases, and the steps recommended by this article should assist in their preservation.

The crux of the potential difficulty lies with the testimonial privileges that require the most stringent form of confidentiality to sustain the status of the privileged information. Whether the courts will view the placement of otherwise privileged communications into computer data bases as a de facto waiver of the privilege will depend on the policy arguments for disclosure of confidential information. To exclude confidential data bases from the trend in favor of disclosure would not broaden or enlarge the scope of the testimonial privileges. These privileges protect the communication of information between those in a special relationship. The information itself is not privileged and may be discovered by other means and in other settings. Treating computer data bases similarly to manual file systems for the purpose of these privileges will not defeat this basic legal premise.

The recommendations suggested in this article are intended to be the reasonable precautions that should be taken to maintain the

199. See supra note 195.
200. See Appendix for suggested language.
testimonial privileges and trade secret protection within a computerized file system. Due to the unsettled nature of the law in the area of privileged communications; it is also suggested that attorneys cautiously utilize computerized filing systems for highly confidential materials.
VI. APPENDIX

NON-DISCLOSURE STATEMENT

This Nondisclosure Agreement is applicable only to (Facility or Site Name), is for a period of ____________ ____________ and shall provide Service Vendor with written notification of expanded applicability if other sites are added. In the event of termination, Service Vendor’s Obligation of Confidentiality shall survive and be binding upon Service Vendor for a period of ____________ after the date of termination.

Service Vendor hereby acknowledges that it may have access to Non-Service Vendor equipment and software at Vendee premises with respect to which Vendee may be under obligations of confidentiality to others, or which may contain confidential proprietary information or trade secrets of Vendee or others. Service Vendor agrees to maintain, and to cause its employees, servants, and agents to maintain the confidentiality of all trade secrets, business or financial or geological information, equipment configurations, software programs and content, and any and all information, data, reports, analysis whatsoever, disclosed or otherwise made available to, or obtained by Service Vendor, its employees, its agents or servants, directly or indirectly, in connection with Service Vendor performing services hereunder, or examining books, records, or equipment of Vendee, its subsidiaries or affiliates, PROVIDED that, Service Vendor shall be under no such obligation of confidentiality with respect to any information in, or becoming a part of, the public domain through no fault of the Service Vendor.

*****

SERVICE VENDOR EMPLOYEE CONFIDENTIALITY STATEMENT

Service Vendor agrees that it shall promptly identify to the Vendee, the names of Service Vendor employees, contractors and agents who will have access to Confidential Information and that Service Vendor shall require each person to provide Vendee a written acknowledgement in the form set forth as an Exhibit hereto that such person has read and understood this Confidentiality Agreement, and personally agrees to comply with the terms thereof.
ACKNOWLEDGEMENT AND CONFIDENTIALITY OBLIGATION

The undersigned hereby acknowledges that he/she has read and understands that certain Confidentiality Agreement dated __________ by ________________ (herein "Service Vendor"). In consideration of the undersigned's employment by Service Vendor and receipt of the Confidentiality Information as described in such Agreement, the undersigned agrees to comply with all the obligations of Service Vendor in such Agreement as fully and to the same extent as if the undersigned were signatory thereto.

Acknowledged and agreed to this _________ day ________________ 19__.

SERVICE VENDOR NAME

Employee Name

Employee Address