The John Marshall Journal of Information Technology & Privacy Law

Volume 4
Issue 1 *Computer/Law Journal - Summer 1983*

Article 6

Summer 1983

Some Aspects of Potential Disclsoure of Confidential Computerized Legal Materials, 4 Computer L.J. 159 (1983)

Reuven R. Levary

Karen K. Duke

SOME ASPECTS OF POTENTIAL DISCLOSURE OF CONFIDENTIAL COMPUTERIZED LEGAL MATERIALS

by REUVEN R. LEVARY* & KAREN K. DUKE**

I. INTRODUCTION

Computers play many roles in the legal profession. They store documents and client files, manage finances, and assist in research. However, "with each step in the development of computer use and sophistication, there has been a parallel rise in more intricate methods by the unscrupulous to use these systems for their own advantage."[1] "The high speed, high volume information processing systems, which increasingly hold law firm data ranging from partnership shares to sensitive litigation documents, now makes it tougher to protect firm and client secrets."[2] The confidential nature of legal work makes the lawyer particularly susceptible to disclosure of computer files either by theft or through the use of the legal process of discovery by opposing counsel. Regardless of the method, the effect is the same: disclosure of the information contained in the attorney's computer system which can prove detrimental to both the reputation of the attorney and to the interests of those who seek his confidential advice.

The future of the legal profession lies in the increased use of computers. The danger of unauthorized access to computer files, however, is real and imminent. Although there is no evidence of a law firm having been the victim of computer theft, "experts are convinced that if they haven't been compromised yet, law firm computers will be hit sooner or later."[3] Indeed, after reviewing security

* Reuven R. Levary is Associate Professor of Management Sciences, School of Business Administration, Saint Louis University, Saint Louis, Missouri.

** Karen K. Duke is a student at the Saint Louis University Law School.

1. Halper, *Lax Controls Over Computers—A Threat to Law Firms*, N.Y.L.J., Apr. 7, 1981, at 3, col. 1.

2. Tell, *Firms Face Computer Theft Issue*, Nat'l L.J., Feb. 22, 1982, at 1.

3. *Id.* at 28.

procedures at a number of major New York law firms, one analyst termed them "sitting ducks" for computer crime.[4] Clearly, the risk of theft can only be effectively combatted if law firms recognize the reasons that their offices are susceptible to theft, isolate the sources of their vulnerability, and take effective steps to protect their files.

This Article will explore the hidden hazards of both legal and illegal computer disclosures. It will evaluate the factors that make revelation of computer-stored data a real threat to lawyers. Finally, this Article will consider the precautions that attorneys can take to shield themselves from computer disclosure.

II. THEFT FROM LAW FIRMS

The legal profession has been spared from computer crime thus far,[5] but the experience of other professions clearly indicates that attorneys' computer files are susceptible to abuse. The potential harm to a client if information stored in the computer concerning a legal action became available to the adversary in the action is readily apparent. A theft of this data would completely undermine the firm's case as the other party would be aware of the intentions of the law firm and be in a position to prepare an answer to every contemplated move.[6]

A. Reasons for Law Firm Susceptibility to Theft

No single factor can be isolated as making the attorney particularly susceptible to theft. A key factor is simply that more law firms are relying on computer technology. Therefore, the problems prevalent in the computer industry as a whole become felt increasingly by the legal profession.

The proliferation of opportunities for computer abuse is due, in part, to the failure of attorneys to comprehend computer technology. The lawyer's blind devotion to the benefits of computerized legal practice creates the risk of theft, since the downside risks of computer use are not thought through.[7] The end result is that it is more difficult for law firms to understand what precautions are necessary to protect their data from misuse.[8] As a consequence, the necessary measures are simply not taken.

If attorney ignorance is a contributing factor in computer crime, the problem is aggravated by the access of increasingly smaller law

4. *Id.*
5. *Id.*
6. *See* Halper, *supra* note 1, at 3, col. 1.
7. *See* Tell, *supra* note 2, at 28.
8. *See* Halper, *supra* note 1, at 3, col. 1.

firms to computers.[9] These attorneys are not only unschooled in computer technology, but also lack the financial means to hire technical experts who can properly use and protect the system.

Computer documents are also more prone to theft simply because computer technology makes data more accessible to would-be thieves. It has been said that "computer files are to paper records as paper records are to stone tablets."[10] Theft from the law office no longer involves gaining physical entry to the effice and then sorting through voluminous documents. Once the thief gains access to the computer system, he need only push a few buttons. In a matter of seconds, the computer will expedite the thief's work by sorting through its files and printing out confidential documents.

The increased use of off-site entry systems makes theft still easier.[11] Off-site entry systems allow the user to make a telephone connection to a computer and to have pertinent data from that computer printed on a conveniently located terminal. Although the thief must still gain access to computer codes, his activities are no longer impeded by the need to gain physical access to the law firm. Thus, rather than the thief going to the computer, the computer files are sent directly to the thief, and his unauthorized access is more likely to go undetected.

> When all record keeping was done by hand, storage could be controlled by locks, guards, electronic eyes and a variety of other methods to keep intruders from the physical presence of the material. The manager/owner of the company could understand all the material in the files and review it visually to determine if it had been altered.[12]

Some authorities maintain that, if properly used, computer systems will increase law firm security. "The nefarious devised methods for opening intricate locks, avoiding electronic eyes, human and animal guards, and dodging pressure sensitive areas"[13] are no longer deemed effective by computer proponents. On the other hand, computer experts note that computer documents cannot be "freely photocopied and inadvertantly fall into the wrong hands."[14] This argument, however, overlooks lawyers' lack of familiarity with computers, and consequently their failure to properly employ the system's safeguards. Even when computers are properly used, the

---

9. *Id.*

10. Price, *Attorney in Discovery May Find Friend in Opponent's Computer*, Legal Times of Wash., May 25, 1981, at 25, col. 1.

11. Halper, *supra* note 1, at 3, col. 1.

12. *Id.*

13. *Id.*

14. Tell, *supra* note 2, at 1.

danger of unauthorized penetration still looms, since access is more difficult to detect. Before law-office computers came into use, firms generally did not maintain backup copies of crucial information in a secure location. Now, because of the computer's vulnerability, double and triple backups are routinely kept.[15] The ease with which computer records may be accidentally destroyed makes duplication imperative, and each additional set of paper records, in turn, becomes susceptible to misuse.

B. Forms of Computer Theft

The methods employed to steal computer documents are as varied as the factors which make law firms susceptible to theft. Indeed, as controls become more sophisticated, so do methods for evading them.[16] Dubbed by some the "computer chamber of horrors," "computer criminals have tapped into data banks, altered computer records, diverted funds, stolen precious computer time, kidnapped data-storage disks, and just plain vandalized computer operations."[17]

Perhaps the most common type of theft is employee embezzlement of funds. The techniques frequently used in other professions to siphon off funds, such as adding nonexistent people to the payroll, are equally applicable in the legal profession.[18] Law firms utilize numerous services, including messengers, investigators, and court reporters. Those with access to computer terminals at large law firms can simply authorize checks as compensation for unused services. Likewise, the trust accounts which are maintained by law firms are equally vulnerable to employee theft.[19] Such accounts, which are kept by law firms in trust for others, are a significant and lucrative aspect of most law practices. They can also prove significant and lucrative to the computer thief who can juggle the computer accounts in his favor. Unlike trust accounts kept by traditional means, the computer embezzler does not make telltale alterations to the records.

The possible uses of raw computer data in the hands of one's opponent are numerous. For example, personnel records, are commonly found in the opposing party's computer system.[20] In a discrimination case, useful information might include each employee's

15. *See* Price, *supra* note 10 at 29.
16. *See* Halper, *supra* note 1, at 3, col. 1.
17. Tell, *supra* note 2, at 28.
18. Halper, *supra* note 1, at 3, col. 1.
19. *Id.*
20. Price, *supra* note 10, at 25.

race, sex, salary, benefits, training and promotional opportunities.[21] Additionally, an adverse party's accounts payable and receivables computer files can reveal much sensitive data. For example, the attorney defending a products liability action may contend that his client was unaware of any defects in the product. The computer files, however, can show otherwise if the client paid refunds to other customers who complained of a defective product.

C. Computer Criminals Within Law Firms

Reported cases of computer theft overwhelmingly indicate that the law firm's own employees are probably its greatest source of risk.[22] In *United States v. Alston*,[23] the defendant and an accomplice deleted adverse information from and added fictitious favorable information to the computerized credit files of individuals who had difficulty obtaining credit. The altered credit files were then forwarded to various lending institutions. Ultimately the applicants were extended loans based on the strength of the doctored credit checks.[24]

Other cases demonstrate that computer theft can occur despite precautions. In *United States v. Sampson*,[25] employees of a NASA facility gained access to the computer system and used computer time for their own purposes. To gain access to the computer, the employees were required to use the necessary code names. It is significant that although NASA projects are considered classified, this unauthorized use went undetected for over seven months.

United States v. Seidlitz[26] demonstrates the degree to which companies are vulnerable to unauthorized computer use by employees. After quitting his job, Seidlitz continued to enjoy unlimited ac-

---

21. By controlling for one variable, such as race or sex, an attorney can explore the differences between promotional opportunities available to one particular class of individuals. *See* Price, *supra* note 10, at 25.

22. The danger of outside appropriation of the computer files of law firms is not as grave as that existing in other industries because the type of information stored in legal computers is of interest to few people. This danger cannot be overlooked, however. Halper, *supra* note 1, at 3. There are numerous cases which demonstrate the vulnerability of computer users to outside appropriation. In *Ward v. Superior Court*, 3 Computer L. Serv. Rep. (Callaghan) 206 (Cal. Super. Ct. 1972), for example, a thief obtained remote access to the computer program of another company, even though numerous safety precautions had been enacted. The thief copied computer programs and used them to get comparable computer programs on the market much earlier than would otherwise be possible.

23. 609 F.2d 531 (D.C. Cir.), *cert. denied*, 445 U.S. 918 (1979).

24. *Id.* at 533.

25. 6 Computer L. Serv. Rep. (Callaghan) 879 (N.D. Cal. 1978).

26. 589 F.2d 152 (4th Cir.), *cert. denied*, 441 U.S. 922 (1978).

cess to his company's system through off-site telephone connections. This was accomplished even though the company used unpublished telephone numbers and secret codes which were discontinued after each employee left.[27]

The legal profession's reliance on a sense of employee responsibility is misplaced.[28] Such confidence overlooks the fact that the industries which have proved vulnerable to employee theft are banking and national defense. These industries and the legal profession share a tradition of confidentiality and trust. Indeed, the ease with which any law firm employee can gain access to computer files is startling. Consultants reviewing law firm security have frequently found that "command codes, program codes and passwords were taped to terminals, making the computer accessible to even the most casual passerby."[29]

D. Effective Security Measures

It is undeniable that individuals with computer expertise who are determined to gain access to the computer system will do so, despite all precautions which may be taken. It is encouraging to note, however, that some law firms that use computers recognize the need for enhanced security. This is evidenced by the fact that 55% of users recently surveyed requested increased security.[30] If law firms institute common sense safeguards, they can deter all but the most resolute computer thief.

Safeguards to minimize the risk of theft should focus on two aspects of the law office: personnel and equipment.[31] Law firms should avoid giving any single employee complete access to the system. At the same time, equipment changes will help to ensure security. All information stored in the computer should be encoded to protect highly sensitive information.[32] Passwords should be required to gain access to each level of information, and particularly sensitive data should be scrambled.[33] Finally, the law firm must remain diligent. Whenever personnel have access to a given level of information, this should be recorded.[34]

---

27. *Id.* at 155.

28. Tell, *supra* note 2, at 28.

29. *Id.*

30. *Id.* at 28-29. Of the security conscious firms, 81% wanted to insulate sensitive programs better, and 62% wanted terminals better guarded against unauthorized use.

31. Halper, *supra* note 1, at 3, col. 1.

32. Tell, *supra* note 2, at 29.

33. Halper, *supra* note 1, at 3, col. 1.

34. *Avoiding Computer Theft*, Nat'l L. J., Feb. 22, 1982, at 28.

III. LEGAL DISCLOSURE—COMPUTER DOCUMENTS AND DISCOVERY

An even more insidious threat to law firms using computers lies in the prospect of legal disclosure through discovery procedures. Discovery is the process by which each side in litigation can determine which witnesses and points of law an opponent will rely upon during trial. The underlying theory is that discovery streamlines the judicial process by eliminating courtroom surprises. Discovery, however, can also create surprises for the attorney who relies on computers to retain privileged information. An attorney may be required to reveal computer stored documents to his opponent before trial, even though the same records, if kept in paper form, would not be subject to discovery.

A. MATTERS PROTECTED FROM DISCOVERY

"Legal" theft involves gaining access to information maintained by the opposing party for purposes of litigation. The issue of discovery of computer-generated or stored documents is complicated. It is well settled, however, that such documents *must* be made available to the opposing attorney unless it can be argued, under limited circumstances, that the information is protected as privileged material.[35] Among the matters generally deemed by the court to be privileged are attorney-client communications[36] and the attorney's work product.[37] Under normal circumstances, the notes which an attorney makes concerning his private conversations with a client and his research and strategy for trial would be shielded from disclosure. When computer use comes into play, however, these rules fall by the wayside.

B. THE ATTORNEY'S DILEMMA

The difficulty which arises from the use of computers is that the privileges that protect paper records from disclosure are not applied in the same manner to computer-generated documents. The attorney-client privilege is supposed to encourage confidential communications between the attorney and client which are related to rendering legal services. To be considered confidential however, the communication must normally take place out of the presence of strangers and in a manner reasonably calculated to be kept secret.

35. Johnson, *A Guide for the Proponent and Opponent of Computer-Based Evidence*, 1 COMPUTER L./J. 667, 686-90 (1979).

36. MO. REV. STAT. § 491.060 (1979).

37. MO. CIV. R. 56.10(b)(3).

Until recently, a major stumbling block with the utilization of computer technology was the fear that the mere use of computers would destroy the privilege since third parties typically encode the information.[38] In *Blue Cross of Northern California v. Superior Court*,[39] however, the court considered this specific issue in the context of the physician-patient privilege. According to the court, the privilege should not be deemed waived simply because third parties have encoded the communication.[40]

The obligation of the computer programmer however, remains unresolved. Attorneys cannot rely on the integrity of such third parties to preserve the rights of their clients.[41] If the programmer reveals the confidential communication to others, the privilege shield may be penetrated. Likewise, the confidentiality of attorney work product is jeopardized when computers are used. An attorney's work product encompasses all pretrial preparation materials. This work product is generally viewed as protected since "proper preparation of a client's case demands that he [the lawyer] assemble information, sift what he considers to be the relevant from the irrelevant facts, prepare his legal theories and plan strategy without undue and needless interference."[42] There is a significant exception built into the privilege, and when computers are used, it frequently tips the scales in favor of disclosure. In this regard, Rule 26(b)(3) of the Federal Rules of Civil Procedure provides:

> [A] party may obtain discovery of documents . . . 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 . . .) only upon 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.[43]

The effect of this rule is to allow opposing counsel to gain access to an attorney's files if counsel can establish that there is no alternative source of information or that such sources are cost prohibitive.

Due to the nature of computer stored information, and since duplication of data gathering constitutes an undue hardship and expense for the opponent, courts are more willing to apply the

38. Lawlor, *Impact of Privilege on Use of Computers by Attorneys*, 5 COMPUTER L. SERV. (Callaghan) § 8-11, art. 2.

39. 61 Cal. App. 3d 798, 132 Cal. Rptr. 635 (1976).

40. *Id.* at 800, 132 Cal. Rptr. at 636.

41. Lawlor, *supra* note 38, at 359.

42. Hickman v. Taylor, 329 U.S. 495 (1947).

43. FED. R. CIV. P. 26(b)(3).

exception and order discovery.[44] For example, computer files which contain computer simulations for use during trial may be discoverable.

> The adverse party is likely to raise objections based on . . . work product, particularly if the simulation has been prepared specifically for the litigation. The modern trend is to permit simulations to be entered into evidence, whether or not the authors intended to introduce them at trial . . . .[45]

Courts reason that the simulation is already prepared and stored in the computer, and to expect the opponent to recreate the analysis is an unreasonable expense.

The key factor tipping the balance in favor of disclosure, despite the confidential nature of the material, is the tremendous cost associated with duplication of the attorney's computer programs. Additionally, the court is less likely to accept the contention of the computer owner that production of the information would be unreasonably burdensome to him. Computers make information more accessible, and consequently less costly for the possessor to assemble when a discovery request is received.[46] Whereas it may take hours to wade through voluminous paper documents to find relevant materials, a computer will require only a few minutes. Furthermore, the lion's share of computer expense is incurred when the raw data is input into the system.[47] Thus, it costs very little for the possessor attorney to make computer stored material available, while it costs considerable amounts of time and money for the opponent attorney to reconstruct the data.

The power of the computer to arrange and sort data already in the system will further tilt the balance in favor of discovery. In certain cases, computers can perform analyses which are not now in existence and which may well prove to be impossible to obtain by other means.[48] In such cases, it clearly constitutes an unreasonable burden to expect opposing counsel to begin the same analysis from scratch.

Case law also indicates that computer-generated documents are likely to be subject to disclosure.[49] In *National Union Electric Corp.*

---

44. Very few computer documents would be immune to discovery request. Rule 26(b)(3), Fed. R. Civ. P. still protects the attorney's "thoughts, mental impressions, conclusions, opinions, and strategies" stored in computer records. *See also* Johnson, *supra* note 35, at 689.

45. Johnson, *supra* note 35, at 696.

46. Price, *supra* note 10, at 26.

47. *Id.*

48. *Id.*

49. *But see* IBM Peripherals, 5 Computer L. Serv. Rep. (Callaghan) 878 (N.D. Cal. 1975). The U.S. District Court refused to exercise its discretion to compel disclosure

v. Matsushitia Electric Industrial Co.,[50] for example, the court held that the requested information was not work product, even though it was developed with the aid of a computer. The court found that the defendants had a substantial need for the computer tape and that the cost to otherwise reproduce the data was prohibitive.[51]

Similarly, in an antitrust action, *Pearl Brewing Co. v. Jos. Schlitz Brewing Co.*,[52] the court held that the program for an econometric model which was prepared for litigation was subject to discovery. The court based its decision on the fact that the hold otherwise would require the defendant's computer and econometrics experts to expend needless hours trying to decipher the meaning of codes in the plaintiff's computer program.[53]

C. Ramifications of Computer Discovery

The possibility of discovery of privileged computer data has significant implications for the use of computers by attorneys. Clearly, computer litigation support systems can be an indispensable tool in complex trials. The computer possesses the power to digest voluminous data and formulate multiple analyses. Due to the danger that unfavorable data will become available to opposing counsel, however, attorneys are well advised that any analyses which are particularly damaging and which are not expected to be used during trial should be erased. Likewise, documents that do not need to be stored in a computer format should be transferred to paper records.[54] The transfer of these documents will afford better protection against discovery requests.

IV. CONCLUSION

The law firm of the future will undoubtedly incorporate computer technology. Accompanying the increased use of computers will be an increased risk of abuse, particularly due to the confidential nature of legal work. Unscrupulous attorneys will attempt to use the opposing attorney's computer system to their own advantage. The end result may be that use of a computer by an attorney

---

of information from a computerized trial litigation support system which was created solely for litigation. The court held that the system reflected the mental impressions, theories and thought processes of the attorney. Significantly, the court held that the documents in question could be obtained from other sources without undue hardship. *Id.* at 879.

50. 7 Computer L. Serv. Rep. (Callaghan) 1181 (E.D. Pa. 1980).

51. *Id.* at 1184.

52. 415 F. Supp. 1122, (S.D. Tex. 1976).

53. *Id.* at 1129.

54. Price, *supra* note 10, at 26.

will prove detrimental to those who seek his advice. In order to effectively use computers, attorneys must be aware of the ever present danger of both legal and illegal theft and must take steps to protect the confidentiality of computer files.