The John Marshall Journal of Information Technology & Privacy Law

Volume 7
Issue 3 *Computer/Law Journal - Summer 1987*

Article 5

Summer 1987

Abuses of Attorneys' Computer Data Bases Threaten Professional Ethics, 7 Computer L.J. 439 (1987)

Debra L. Bray

ABUSES OF ATTORNEYS' COMPUTER DATA BASES THREATEN PROFESSIONAL ETHICS

The legal field is now subject to computer abuses which have plagued the general business world. Attorneys are using computers to store confidential information, perform legal analysis, and generate legal documents.[1] Such use creates a risk that files and confidential information stored in computers will be subject to a variety of computer abuses, including unauthorized access, theft, alteration or destruction—problems widely publicized within the business world. [2] Attorneys have a professional responsibility to maintain the confidentiality of client data. Failure to do so may harm a client or benefit unscrupulous third parties. Many law office computers, however, have no protections, or inadequate protections, against computer abuses.[3]

This Note will examine the general problem of computer abuse and the potential for such abuse in the legal field. Computer abuse is defined in this Note as any unauthorized access to, or use of, a computer or its data bases.[4] Computer abuse has traditionally involved the theft

1. Poore & Brockman, *The Threats to Computer Security*, NAT'L L.J., Oct. 14, 1985, at 14, col. 1; *see, e.g.*, Pearl Brewing Co. v. Joseph Schlitz Brewing Co., 415 F. Supp. 1122, 1134 (S.D. Tex. 1976) (using a computer generated econometric model in anti-trust litigation); Honeywell Inc. v. Sperry Rand Corp., 180 U.S.P.Q. 673 (D. Minn. May 26, 1976) (using numbered narrative statement, designated supporting and opposing evidence, and cumulative lists and indices of exhibits generated and maintained in computer storage); IBM Peripherals, 5 Computer L. Reporter 879 (N.D. Cal. 1975), (using a computerized trial support system); ABA Comm. on Ethics and Professional Responsibility, Informal Op. 1364 (1976) (use of an outside data processing firm); Soma & Youngs, *Confidential Communication and Information in a Computer Era*, 12 HOFSTRA L. REV. 849 (1984).

2. *See generally* Whalen v. Roe, 429 U.S. 589 (1977); *Computer Crime: Hearing Before the Subcomm. on Civil and Constitutional Rights of the House Comm. on the Judiciary*, 98th Cong., 1st Sess. (Nov. 18, 1983); *Privacy and 1984: Public Opinions on Privacy Issues: Hearing Before the Subcomm. on Gov't Information, Justice and Agriculture of the House Comm. on Gov't Operations*, 98th Cong., 1st Sess. (Apr. 4, 1984) (hereinafter *Privacy Hearing*); D. PARKER, S. NYCUM & S. OURA, COMPUTER ABUSE (1973); Note, *Computer Abuse: the Emerging Crime and the Need for Legislation*, 12 FORDHAM URBAN L.J. 73 (1984); Clymer, *Privacy Threats Worry Americans*, N.Y. Times, Dec. 8, 1983, at D24, col. 1.

3. Poore & Brockman, *supra* note 1, at 14, col. 1.

4. For a variety of definitions of computer abuse, see Note, *supra* note 2, at 74-75 (1984).

of data, unauthorized use of computer software and equipment, embezzlement of tangible and intangible assets, destruction of computer data or equipment, and ransoming of computer assets.[5] Attorneys who use computers, especially computers which can be accessed by unauthorized individuals through the telephone lines, could be subject to any of these illegal practices. Most troubling, however, is the potential attack on stored information. Information storage and manipulation are the most prevalent purposes for which attorneys use computers. Unwarranted disclosure, alteration, or destruction of this vital, and often confidential, information can harm clients.

The legal system supports and relies upon strict confidentiality and accurate detail. This Note will describe current confidentiality requirements for attorneys, sanctions which can be imposed upon attorneys for failing to reasonably protect confidential data, and sanctions which can be imposed upon individuals for the unauthorized access, theft, alteration, or destruction of confidential information. It will then suggest that neither current confidentiality requirements, nor criminal and civil sanctions adequately protect clients from the abuse of confidential information when lawyers use computers. This is especially true when computers can be accessed through the telephone lines. Finally, this Note will recommend further protections and means of implementation.

I. COMPUTER ABUSE

A. GENERAL BUSINESS ABUSE

Computer abuse is a serious and increasing problem, yet there are no reliable statistics regarding the frequency or severity of such occurrences.[6] Developing complete and reliable statistics on computer abuse is difficult for several reasons. First, computer abuses are often undetected and, therefore, unreported. Even when abuse is discovered, many businesses do not report it because they want to avoid disclosing to the public the vulnerable aspects of their computer systems. They fear making future attacks upon their own computer easier for others. Second, businesses fear that publicity about computer abuse techniques might encourage and increase such abuse overall. Third, most crime statistics are gathered from police arrest or conviction records.[7] Computer abuse has been prosecuted under numerous statutes, including fraud and wiretapping, not traditionally associated with computer abuse. Thus, statisticians would have the laborious task of sifting

5. D. PARKER, *supra* note 2, at 91-112.

6. BUREAU OF JUSTICE STATISTICS, U.S. DEP'T OF JUSTICE, COMPUTER CRIME: COMPUTER SECURITY TECHNIQUES 1 (1982).

7. *Id.*

through individual crime reports to find computer crime information and, even then, some crime reports might omit such details.

Studies show that types of computer abuse vary greatly, and that the amount of harm from such abuse is significant. A study conducted at Stanford University collected and attempted to verify reports of computer abuse.[8] The study revealed that most businesses have experienced problems involving vandalism, theft of information or property, fraud, or unauthorized use, access, or sale of computer time or data.[9] Some examples from this study illustrate the nature of the problem: (1) "Programmer altered a program to cause a computer to print fictitious credit notes for cigarette coupons and sent to his address;"[10] (2) "Computer operators of a consulting firm rendered useless the subscription list of a magazine;"[11] (3) "An employee destroyed on-line data files after being given notice of termination;"[12] (4) "A former employee of a time-sharing service is alleged to have made unauthorized access to extract confidential data over a long distance circuit from Cincinnati;"[13] (5) "Two employees of a U. S. economic data collection firm extracted and sold data;"[14] (6) "Students held the Atomic Energy Commission computer for $100,000 ransom."[15]

In acts of crimes or abuse, computers serve as the target, tool, accomplice, or scapegoat.[16] Protections should address all forms of attack, since each can be equally harmful to the businesses and clients involved. As a target, a computer's programs and data may be stolen, vandalized, or simply used without authorization. As a tool for access and transfer, a computer facilitates the commission of crimes, such as theft or embezzlement. As an accomplice, the computer does not participate in, but is used to plan the commission of a crime. Finally, as a scapegoat, a computer is simply blamed for wrongful acts to avoid the wrongdoer's personal responsibility.

Statistics reveal that computer abuse exists in each of the above forms. Only the first, computer as a target, relates specifically to the threat to confidential information maintained in attorneys' computers. The future, however, promises more extensive application of computers in business and in the legal field. More computer network systems will be used, and more transactions will be conducted between computers

8. D. PARKER, *supra* note 2.
9. *Id.* at 14-17, 91-112.
10. *Id.* at 93.
11. *Id.* at 95.
12. *Id.* at 94.
13. *Id.* at 96.
14. *Id.* at 100.
15. *Id.* at 94.
16. *Id.* at 30-33.

rather than between people. Attorneys will undoubtedly be involved in all of these aspects on behalf of their clients, and risks that perhaps do not currently exist will arise in the future. Business people, attorneys, and policy makers must plan for this expansion, and develop protections for all forms of abuse.

B. POTENTIAL FOR ABUSE IN THE LEGAL FIELD

Information becomes valuable to others when it can be used to make a profit, increase power or control over others, enhance political advantages, give voice to a complaint or vindicate a perceived wrong, or increase the effectiveness of an overzealous employee.[17] Information that does not appear on its face to create a target for computer abuse may actually do so because of its confidential character. If the information is private or confidential, clients may feel embarrassed by disclosure, lose a strategic advantage, or even lose a lawsuit in which they otherwise would have prevailed.

In the course of seeking effective representation, clients must often give attorneys information that they would not want others to have. Examples of such information include addresses and telephone numbers, financial information, trade secrets, tax and business planning information and other confidential or secret data. Such information could be valuable to others for any of the reasons mentioned above. Furthermore, such information, and the work product and strategic planning conducted by the attorney, would be especially valuable to an adversary. Although attorney work product is not available to an adversary through the normal discovery process, an unscrupulous attorney could acquire the opposition's confidential records through illegal computer access. Such knowledge would unfairly benefit the unscrupulous attorney's client to the detriment of the opposing party. There is no reason to believe that the legal profession will be, or is, immune from computer abuses.

The United States Department of Justice has attempted to identify some special risks involved in individual applications of computers.[18] Some of the special risks that apply to computer systems used by attorneys, because of the value of the stored information, are intentional or accidental disclosure, modification, and destruction or use of personal or sensitive data, records, or trade secrets. The violation of confidentiality rules, personal data regulations and privacy laws were also identified.

---

17. A common example is the unauthorized transfer of funds through illegal access to bank computers. Opportunities for such illegal use of computers will continue to increase as computer applications expand. R. TURN, PRIVACY AND SECURITY IN PERSONAL INFORMATION vi (1974).

18. BUREAU OF JUSTICE STATISTICS, *supra* note 6, at 10-11.

The threat to computer confidentiality may even be greater in the legal field than in general business. Attorneys are generally unfamiliar with computer processes or security, and often do not use a computer security system at all.[19] The Department of Justice reported that "dangers lurk not where losses have been anticipated and good controls exist, but where vulnerabilities have not been anticipated and controls are lacking."[20] The problem is that security "cost[s] money without visible, direct contributions to performance."[21] It is difficult to convince some people that a potential for harm is a sufficient reason to take action. This was a primary issue in the Federal computer crime legislation debate.[22] Opposing parties or counsel, investigators, or unrelated persons who feel that the information might benefit them could access a client's personal or confidential data. A recent survey revealed that forty-five percent of known computer abusers were either competitors or unrelated, unknown individuals.[23]

Computers also increase the risk that employees or previous employees may steal, modify, or divulge information. As opposed to computer files, paper files are much less accessible and amenable to interpretation and collation. It is more difficult to detect the existence of data in a paper file because physical searching is necessary. It is also more difficult to gain access to physical files maintained in varied and locked locations. Furthermore, it is more difficult simply to assimilate and interpret data when it is in a raw, hard file form.[24] A disgruntled or unscrupulous employee or former employee is able to alter, copy, or steal information more easily when it is in the form of computer data. But why would this occur? The motivations are unlimited: anger at a client or the attorney, promise of financial gain (for example, by selling the information or using the information to blackmail someone), promise of strategic advantage (advance notice of an investment opportunity or political use), the simple challenge of it, or even overzealousness.[25]

Another area vulnerable to abuse in attorneys' computer use involves the transmission of data. Abusers can intercept or eavesdrop when computer data is sent over the telephone lines to other computer terminals.[26] This type of computer abuse, whether intentional or inadvertent, results in an unauthorized person possessing the information.

---

19. Poore & Brockman, *supra* note 1, at 14, col. 2.

20. BUREAU OF JUSTICE STATISTICS, *supra* note 6, at 4.

21. *Id.* at 3.

22. *Privacy Hearing*, *supra* note 2, at 2.

23. Task Force on Computer Crime, *Report on Computer Crime*, 1984 A.B.A. SEC. CRIM. JUST.

24. R. TURN, *supra* note 17, at 2.

25. *See generally id.* at vi.

26. M. SCOTT, COMPUTER LAW § 7.41 (1984).

The sender may not even be aware that that person has gathered the information.

Some hypothetical situations, drawn from reported computer abuse in other fields, will clarify the types of risks attorneys face. First, Secretary has been offered $10,000 for a list of names and addresses of all of the attorneys' clients. This will benefit Third Party who will use the information to prepare a mailing list to advertise and solicit sales for a product or service. Secretary can obtain the list by pushing just a few computer keys. The list is prepared and delivered; the abuse is undetected by the attorney and her clients. The Internal Revenue Service only incidentally discovers the abuse when investigating the unreported receipt of money by Secretary. Client's privacy interests have been invaded, and would have gone undetected.

Second, Investigator has been hired to discover an individual's assets. She gains access to tax planning strategies and confidential information in an attorney's computer through the use of a modem and the telephone lines. Several bank accounts and interests in land are discovered and used by Third Party. Client's privacy and perhaps financial interests have been harmed, but the unauthorized access is not detected.

Third, Computer Programmer has just been given notice of termination, is angry, and programs that computer to destroy all client files one month after she has gone. The program is not discovered until after all of the information is lost.

Fourth, Unscrupulous Attorney is involved in a complex lawsuit which, if won, could recover millions of dollars for her client and a substantial contingency fee for the law firm. Attorney knows that Defendant's Lawyers have been using a computer to strategize and organize masses of critical information. Some of the information has been obtained through the discovery process, but Defendant's Lawyers' work product is not discoverable. Attorney has a home computer with a modem, has taken a few computer courses in college, and knows that she can gain access to the information through the telephone lines with only an access code. She programs her computer to try all permutations of numbers until the correct code is discovered. As expected, Attorney gets all of the information. The defendant and the legal system have been violated.

The risks of abuse increase with the widespread use of computers, and the use of small, dedicated computers, called modems, which link data communication circuits. "By proper utilization of modems . . . and ordinary telephone lines, it is possible to establish powerful . . . networks of . . . computers."[27] Small office and home computers, in numbers estimated at five million for 1985, can be connected to telephone

27. D. PARKER, *supra* note 2, at 21-22.

computer networks.[28] A user need only know, or discover through trial and error, a telephone number and access code to access a computer through a modem.[29]

II. CURRENT REQUIREMENTS OF CONFIDENTIALITY

Confidentiality is at the core of an attorney's duty. Canon 4 and ABA Model Rule 1.6[30] require that attorneys maintain their clients' confidences and secrets. Confidences are communications received from a client in the course of the attorney-client relationship, and are also protected by the law of attorney-client privilege. Secrets are information about a client gathered during representation. There are few exceptions to the confidentiality rule.

There are two basic rationales for requiring confidentiality. First, it is presumed that the advocacy system operates best when both sides are advocating and presenting their positions fully. Attorneys must have all relevant information to best represent the interests of their clients.[31] Without the full story, attorneys cannot represent clients to the clients' utmost advantage. Confidentiality is necessary because clients would otherwise withhold information that they believed was harmful.

Second is a dignity rationale. Clients' dignity is furthered when their attorneys act completely in the clients' interest. Society values highly dignity and autonomy; the law must give preeminence to these values. The attorney acts as a friend of clients, giving clients dignity.[32] This dignity is further strengthened by the assurance of complete confidentiality.

The professional codes and rules governing attorneys are enforced by the state bar in each state and, in some circumstances, by the courts. Neither the Model Rules nor the Model Code[33] set forth any guidelines for protecting confidential information maintained in computers. Such protection has been left to the discretion of attorneys within the general bounds of confidentiality requirements.

It is the ABA's policy to interpret standards to permit (1) the use of modern business practices, and, (2) assuming that reasonable care is

---

28. *Federal Computer Systems Protection Act: Hearing on HR 3970 Before the Subcomm. on Civil and Constitutional Rights of the House Comm. on the Judiciary*, 97th Cong., 2d Sess. 11 (daily ed. Sept. 23, 1982). (William A. Bayse, Assistant Director, Technical Services Division, Federal Bureau of Investigation) [hereinafter *Protection Act Hearing*].

29. M. SCOTT, *supra* note 26, § 1.9.

30. MODEL RULES OF PROFESSIONAL CONDUCT Rule 1.6 (1983).

31. People v. Belge, 372 N.Y.S.2d 798 (1975).

32. C. Fried, *Lawyer as Friend: The Moral Foundations of the Lawyer-Client Relationship*, 85 YALE L.J. 1060-89 (1976).

33. MODEL CODE OF PROFESSIONAL RESPONSIBILITY (amended 1982).

taken, the use of computers.[34] For example, the ABA has decided that attorneys have no duty to inform their clients that an outside computer agency will be used and will have access to clients' confidential data.[35] It is clear, however, from the ABA and various state bar opinions involving computer use, that balancing the problem of computer abuse, confidentiality, and efficiency has been difficult and may not yet be settled.

III. CURRENT PROTECTIONS AND SANCTIONS

A. PROTECTIONS AND SANCTIONS AGAINST ATTORNEYS FOR FAILING TO TAKE ADEQUATE PRECAUTIONS

There are some sanctions which can be imposed on attorneys that fail to take reasonable precautions to protect confidential client data. State agencies which license attorneys have the power to impose sanctions upon attorneys for failing to act in accordance with professional codes and rules.[36] The major flaw in this protection, is that a large percentage of computer abuse is never detected.[37] The ability to impose sanctions requires the detection of abuse. Detection requires effective auditing of attorney's security provisions, and this is currently not done.

The common law also provides a cause of action in tort for the negligent use of a computer. Those who use computers must do so with care.[38] A client who has suffered from a lack of computer protections would have to establish all of the elements of a cause of action in tort, including duty, breach of duty, causation and damage.[39] To do so, a client must be aware that some computer abuse has occurred. As with protection through required confidentiality, protection through tort law is dampened by the low probability of detecting computer abuses. Clients cannot prove a tort lawsuit without detecting the abuse; in fact, they would not even know to initiate the lawsuit. Further, some types of harm would be difficult to value, such as invasion of privacy.

The risk of a malpractice lawsuit is another potential protection for confidential computer information. Attorneys must maintain the same standard of care as similar professionals.[40] Courts sometimes use a reasonable conduct standard and, other times, an ordinary conduct stan-

34. ABA Comm. on Ethics and Professional Responsibility, Informal Op. 1127 (1970). *See also* ABA Comm. on Ethics and Professional Responsibility, Informal Op. 1364 (1976).

35. *Id.*

36. MODEL RULES OF PROFESSIONAL CONDUCT, Scope (1983).

37. *See supra* text accompanying notes 26-27.

38. M. SCOTT, *supra* note 26, § 7.18.

39. M. SCOTT, *supra* note 26, §§ 7.2, 7.7-7.18.

40. BUREAU OF JUSTICE STATISTICS, *supra* note 6, at 17-19.

dard.[41] An ordinary conduct standard would not provide much protection at present, since many, if not most, attorneys have inadequate security protections. The reasonable conduct standard could provide some protection, but the lack of reasonable care in providing computer security would have to be discovered. This would not occur unless some computer abuse was discovered, an event that is often unlikely. Michael D. Scott further contends that the courts are not prepared to deal with computer issues.[42] Judges may know so little about computers, computer security devices, and computer abuse that they may be reluctant to find an attorney guilty of malpractice for a similar lack of knowledge in a technical area. On the other hand, judges routinely find malpractice in medicine and automotive design with a similar lack of technical knowledge.

Finally, even if an attorney is ultimately sanctioned for inadequately protecting client confidences and secrets, the client has been harmed and one of the legal system's core requirements compromised. The legal profession must follow some reasonable standards to protect confidential data before harm has occurred, and this is not a current practice.

B. SANCTIONS AGAINST COMPUTER ABUSERS

There are criminal sanctions which can apply to computer abuse, and these can be used potentially against individuals who unlawfully access attorneys' computers. A few states have specific computer crime statutes,[43] but most computer abuse must fit into other crime categories.[44] Access to a computer by improper means to commit a criminal act is a crime in some states.[45] There are also some federal criminal statutes under which computer abuse sanctions could be sought, including wire fraud statutes, embezzlement, and theft statutes.[46]

The current criminal laws' inadequacy in dealing with computer abuse in all of its forms has been widely discussed.[47] When the issue regarding which statute the computer abuse might be prosecuted under arises, however, the client has already been harmed. Since confidential-

41. McLean v. Rankin, 41 Or. App. 3, 596 P.2d 1329 (1979).

42. M. SCOTT, *supra* note 26, § 1.4.

43. M. SCOTT, *supra* note 26, § 8.17. For a specific example of a computer crime statute, see Cal. Penal Code § 502 (West Supp. 1983).

44. M. SCOTT, *supra* note 26, § 8.5.

45. M. SCOTT, *supra* note 26, § 8.18. Examples include theft, telephone abuse, and malicious mischief. *Id.*

46. 18 U.S.C. § 1343 (1982); 18 U.S.C. §§ 641, 659 (1976).

47. D. PARKER, *supra* note 2, at 5-6, 55-59; Peck, *Extending the Constitutional Right to Privacy in the New Technological Age*, 12 HOFSTRA L. REV. 893 (1984); *Protection Act Hearing*, *supra* note 33, at 3.

ity is a core requirement of the legal profession,[48] and is necessary to protect the system and the dignity of the individuals involved,[49] protection should not be left to the mere possibility that the criminal penalties may deter some criminals, even if obscurities in the criminal codes did not exist. Furthermore, there is the ever present risk that computer abuse will not be detected, or could not be proven against particular individuals.

Potential tort claims to remedy the effects of computer abuse include conversion, interference with economic relations, fraud, and invasion of privacy.[50] Pursuing rights under tort law involves the problem that the tort may not be discovered. Furthermore, costs of pursuing legal action can be prohibitive. In addition, damages may neither (1) reflect the total harm to the client (for example, embarrassment), (2) reflect the harm to the legal system, nor (3) be sufficient to deter the particular computer abuser.

The federal legislature has recognized the problems inherent in relying upon deterrence from criminal and civil penalties to curb computer abuses and protect privacy, and has enacted legislation to protect individuals in a few areas. Legislation aimed at protecting individuals from computer abuses before they occur includes the Fair Credit Reporting Act[51] and the Privacy Act.[52] There is also legislation governing financial institutions.[53] The Fair Credit Reporting Act was enacted to ensure that consumers are treated with fairness, impartiality and privacy.[54] It states that "an elaborate mechanism has been developed for investigating and evaluating the credit worthiness, credit standing, credit capacity, character, and general reputation of consumers."[55] The fear of computer abuse was a motivating factor in bringing about the legislation. Some of the protections provided by these Acts include limited dissemination and protection from unauthorized access, the right to know that data is being maintained, and the right to access and challenge data. These protection requirements have been codified into law despite computers in these fields having had consistent security protections.

---

48. *See supra* text accompanying notes 30-32.

49. *See supra* text accompanying notes 31-32.

50. M. SCOTT, *supra* note 26, § 7.3.

51. Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681t (1976).

52. Privacy Act of 1974, 5 U.S.C. § 552(a) (1974 & Supp. IV (1980)).

53. Financial Institutions Regulatory & Interest Rate Control Act of 1978, Pub. L. No. 95-630, 1978 U.S. CODE CONG. & ADMIN. NEWS (92 Stat. 3641) 9273, 9305-06.

54. Fair Credit Reporting Act, *supra* note 51, § 1681(4).

55. *Id.* § 1681(2).

IV. PROPOSED PROTECTIONS

Computers should not be used to manipulate and store private or confidential information unless adequate security protections are afforded. Rein Turn describes the adverse effects that computer abuse can have upon victims.[56] These include harm to a person's physical safety, well-being, self-respect, solitude, liberty, right to refrain from self-incrimination, mental well-being, privacy, strength of character, economic security, and opportunities. Society must balance legitimate business and information needs against protection of private and confidential information and the possibility of harm. A line must be drawn to establish the appropriate level of protection between the two extremes—i.e., prohibiting maintaining information in computer data banks versus allowing complete freedom to store and manipulate information without protection requirements.

This balancing process requires that a realistic value be placed upon the information. A sensitivity scale should take factors such as type of information, potential value to others, potential harm from unauthorized disclosure, use, or manipulation, and the purpose or need for keeping the information in the computer into account. Other factors that may be useful in drawing this line include customer or client consent, value of the good or service provided, and legal or professional requirements.

There are only a few instances in which absolute protection of confidential or private information should be given. Justice Brennan stated in his *Whalen v. Roe*[57] concurrence that the advancement of computer technology might necessitate a judicial curb on that technology. He further stated, however, that reasonable security protections usually were sufficient.[58] The Court noted that the right to collect and use information through computers is usually accompanied by a statutory or regulatory duty to avoid unwarranted disclosure.[59]

The balancing cannot be left completely to each attorney. The risks are too great that individuals and the system may be harmed. The United States Department of Justice has recommended using a baseline concept for establishing computer security protections.[60] A basic level of protection should be set which all attorneys would be required to meet. Security levels below the baseline would place a stringent burden upon the attorneys to prove adequacy. For example, a baseline could require that all attorneys place confidential information into their com-

56. R. TURN, *supra* note 17, at 29.
57. 429 U.S. 589 (1977).
58. *Id.* at 607.
59. *Id.* at 605.
60. BUREAU OF JUSTICE STATISTICS, *supra* note 6, at 35-36.

puters in code. The information could, therefore, not be read by unauthorized individuals unless they could first access the information, and then decipher it. Any attorney not complying with this baseline requirement would be presumed to be in violation of the law unless the attorney showed that the security protections afforded were sufficient (or superior to placing the information in code form). The baseline, however, would be a minimum guide for attorneys generally unfamiliar with computer security techniques. Further suggestions for protections would be provided to bring the risks to a reasonable level. For example, if unauthorized disclosure would be extremely harmful to a client or if the information were very valuable, a reasonable level of protection might require further limitations.

The baseline should be developed by a task force composed of computer experts and legal professionals, in a manner similar to that recommended for in-house security reviews.[61] The task force should serve to review and identify general assets subject to loss, their value, the consequences of loss, the types and level of risk, available protections and their effectiveness, and alternative means of storing and manipulating the information. It should consider all threats, intentional, accidental, or negligent intrusion, destruction or manipulation of data, and inappropriate data integrity. Once the baseline is established, periodic, random reviews of attorneys' computer security techniques should be made to assure integrity. The baseline, with reviews, would require more monitoring of computer security than one mandatory level of security would, but the variation among risks is too great to establish a single level of protection. Overprotection would be inefficient, and underprotection would unreasonably risk information exposure or tampering.

The following protection factors should be included in the reviews and baseline: (1) safeguards including notification of the existence of the data base and the rights to inspect and amend; (2) procedures for maintaining confidentiality, including increased anonymity, access control, and reduced exposure by collecting only necessary information; (3) data security techniques including defensive hardware and software, control over users' actions, and the use of cryptography in data files and communication links; and (4) integrity management including procedures for detecting errors and testing all systems.[62]

Attorneys should be required by law to safeguard their clients' rights when computers contain clients' private and confidential information. Attorneys should inform their clients regarding what information will be placed into computer data banks, and what types of security

61. BUREAU OF JUSTICE STATISTICS, *supra* note 6, at 12.

62. D. PARKER *supra* note 2, at vii-ix.

measures will be used. Clients would then have the option of approving the plan, negotiating with the attorney about parts of the plan, or choosing another attorney. Clients should always have the right to review and correct any data. Such a client right also benefits attorneys who must have reliable and complete information to adequately represent a client's interests.

Procedures for maintaining confidentiality and data security techniques should vary, depending upon the sensitivity of the data to be stored. The baseline would apply, and auditing would confirm necessary protections.

Maintaining data integrity is also important. Attorneys should be required to maintain hard files to correct errors in the data base or replace information which might be accidentally or purposefully destroyed, altered, or improperly entered. Furthermore, attorneys should make periodic reviews of the computer programmers' work and methods.

A thorough analysis of any security device should also consider components such as probability of deception, resistance to manipulation, resistance to circumvention, detection, and time to detect.[63] Protections must span all steps of data manipulation from input to storage and transmittal. Auditing must be done by a responsible, knowledgeable, and detached agency.

Some specific security controls have been identified by the Department of Justice.[64] Procedures to assure data integrity include staff accountability and usage rights for all data and data manipulation, confirmation of receipt of hard copies, accountability for the accuracy, safekeeping, and dissemination of data, suppression of incomplete and obsolete data, and destruction of discarded hard copies. The physical security of the computer hardware and software should be provided by locking doors, and, where necessary, guarding the interior. Access to the areas where computers are kept should be minimized and, for some sensitive types of data, sign-in and sign-out procedures should be implemented.

Operations security provisions should include computer systems activity records, minimizing copying of sensitive data, employee identification on work product, data file and program backup, and backup of power source. It would also be necessary to confirm trustworthiness of employees.

Access controls could include elimination of dial-up access to the computer, limiting dial-up access to regular business hours when responsible employees are present, removing sensitive data from dial-up

63. R. TURN, *supra* note 18, at 60-61.

64. BUREAU OF JUSTICE STATISTICS, *supra* note 6, at 12.

access, implementing log in procedures, and limiting availability of the telephone access numbers. Computer access and use should be monitored. If access is made, the computer should record automatically the relevant identification. Finally, passwords should be used to further protect sensitive data. These should be changed regularly and issued discretely. Records of the passwords within the computer system should be individually encrypted.

V. IMPLEMENTING PROTECTIONS

The Federal government should enact legislation requiring attorneys to implement computer security protections when any confidential, private, or secret information involving a client is placed in the data base. Actual development of a baseline, as discussed earlier, and enforcement should be done by a task force, set up by the government. There is strong federal and public interest in this area. Loss of privacy and confidentiality in legal services would detrimentally affect the advocacy system in the United States,[65] as well as pose a threat to liberty, autonomy, self-hood, and other human values.[66] The public has voiced its concern in opinion polls about the effects of computers on privacy and confidentiality.[67]

Uniformity is also necessary and would require federal action. Interstate commerce relies upon the effective enforcement of laws, legal rights and obligations. Lawsuits often involve individuals and businesses from different states. Individuals or businesses may have to hire lawyers from other states to represent them. Differences among the states in computer security requirements could adversely affect the rights and interests of individuals and businesses. For example, a client might hire a lawyer from another state, thinking that the lawyer is subject to the same computer security requirements as exist in the client's own state. The client might therefore feel secure in divulging some very sensitive data to the attorney to be placed into the computer data banks. In reality, the attorney's state may not require any security devices. The information, which the client thought would be protected, would not be secure.

The integrity of the Federal Court system is also the responsibility of the federal government. Confidential information and attorney work product must be protected for the reasons discussed in Section II of this Note. The federal government cannot rely upon individual state protections; some states might not take any action to require security.

An alternative to federal legislation would be for the government

65. *See supra* notes 30-35 and accompanying text.

66. Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 423 (1980).

67. *Privacy Hearing*, *supra* note 2, at 4-7.

to appoint a task force to establish standards and develop a model act which could be adopted by the states. This alternative, however, could compromise uniformity and threaten security because states are not required to adopt model acts.

CONCLUSION

The legal field is subject to the increasing abuse of computer data bases, thus exposing confidential and private information to unauthorized individuals. This threatens the legal system and the privacy, autonomy, and liberty of individuals. Attorneys have sometimes failed to protect computer data, and generally lack sufficient familiarity with computer processes and potential abuses to develop adequate protections. Furthermore, because protections are expensive, attorneys may not develop protections against potential harms without government intervention. This Note has suggested that the Federal Government has an interest in protecting privacy and the legal system, and should therefore investigate and establish security protection baselines and audit computer systems used by attorneys.

Debra L. Bray